IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

IN RE CROWDSTRIKE HOLDINGS, INC. SECURITIES LITIGATION	Civil Action No. 1:24-cv-00857-RP **CLASS ACTION** **DEMAND FOR JURY TRIAL**

CONSOLIDATED CLASS ACTION COMPLAINT FOR VIOLATIONS OF THE FEDERAL SECURITIES LAWS

TABLE OF CONTENTS

I. INTRODUCTION 1

II. JURISDICTION AND VENUE 7

III. PARTIES 8

IV. SUMMARY OF THE FRAUD 9

A. CrowdStrike's Purported Compliance With Industry Standards And Federal Requirements Concerning Quality Assurance For Software Updates 9

1. Basic Quality Assurance Processes Are Critical To Companies Like CrowdStrike That Remotely Update Customer Software 11

2. CrowdStrike Consistently Assured Investors That Its Software Update Process Was Consistent With Industry Standards And Federal Compliance Requirements 22

B. Unknown To Investors, CrowdStrike Failed To Conduct Necessary Tests Of Software Updates, Roll Out Updates In Phased Releases, And Otherwise Comply With Industry Standards And The Government's Requirements 29

C. CrowdStrike Crashes Millions Of Systems Worldwide, And Customers And Investors Learn That CrowdStrike Failed To Sufficiently Test And Secure Its Falcon Updates 38

D. Investors Suffer Losses When They Learn That CrowdStrike Failed To Sufficiently Test And Secure Its Falcon Updates 45

E. CrowdStrike Admits That It Failed To Conduct Necessary Tests And Secure Its Falcon Updates, Leading To Even More Investor Losses 47

V. ADDITIONAL ALLEGATIONS OF SCIENTER 52

VI. DEFENDANTS' FALSE AND MISLEADING STATEMENTS AND OMISSIONS DURING THE CLASS PERIOD 64

A. FALSE AND MISLEADING STATEMENTS IN 2022 65

1. September 2022 Fal.Con Conference 65

B. FALSE AND MISLEADING STATEMENTS IN 2023 66

1. April 2023 "Investor Briefing" 66

2. August 30, 2023 Earnings Call 67

3. September 2023 Goldman Sachs Investor Call 67

4. November 2023 Earnings Call 68

5. December 2023 Interview of Kurtz 69

C. FALSE AND MISLEADING STATEMENTS IN 2024 70

1. April 2024 CrowdStrike Video Presentation 70

D. FALSE AND MISLEADING STATEMENTS IN ANNUAL SEC FILINGS 71

1. Form 10-K Annual Reports 71

2. Annual Proxy Statements 72

E. FALSE AND MISLEADING STATEMENTS ON CROWDSTRIKE'S WEBSITE 72

VII. DEFENDANTS' MISLEADING STATEMENTS AND OMISSIONS WERE MATERIAL TO INVESTORS 75

VIII. LOSS CAUSATION 78

IX. INAPPLICABILITY OF THE STATUTORY SAFE HARBOR 84

X. PRESUMPTION OF RELIANCE 85

XI. CLASS ACTION ALLEGATIONS 86

COUNT I 89

For Violations of Section 10(b) of the Exchange Act and SEC Rule 10b-5 Thereunder (Against All Defendants) 89

COUNT II 91

For Violations of Section 20(a) of the Exchange Act (Against Defendants Kurtz and Sentonas) 91

XII. PRAYER FOR RELIEF 93

XIII. JURY DEMAND 93

Lead Plaintiff Thomas P. DiNapoli, Comptroller of the State of New York, as Administrative Head of the New York State and Local Retirement System, and as Trustee of the New York State Common Retirement Fund ("New York State Common Retirement Fund"), by and through its undersigned counsel ("Lead Counsel"), brings this action under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 (the "Exchange Act"), and U.S. Securities and Exchange Commission ("SEC") Rule 10b-5 promulgated thereunder, against Defendants CrowdStrike Holdings, Inc. ("CrowdStrike" or the "Company"), its Chief Executive Officer, George Kurtz ("Kurtz"), and its President, Michael Sentonas ("Sentonas") (collectively, the "Defendants"), on behalf of itself and all other similarly situated persons or entities who purchased or otherwise acquired CrowdStrike common stock between September 20, 2022 and July 30, 2024, inclusive (the "Class Period"), and were damaged thereby (collectively, the "Class").

I. INTRODUCTION

1. During the Class Period, CrowdStrike was one of the world's fastest-growing cybersecurity companies. CrowdStrike secured contracts with the U.S. federal government, 43 state governments, and over half of all Fortune 500 companies to purchase its one and only product, CrowdStrike's "Falcon" cybersecurity platform. According to CrowdStrike, what set Falcon apart from competing products was its "Rapid Response" updates, which were delivered silently to CrowdStrike's customers through the "cloud" and included the latest threat detection code. While customers and investors applauded the functionality of Falcon's software, they were concerned that its software updates may, themselves, be unstable because (unlike traditional software updates) the Rapid Response updates were installed on customers' computers without notice. In response to these concerns, CrowdStrike, its CEO, Defendant Kurtz, and its President, Defendant Sentonas, represented over and over that it adhered to industry-standard testing and quality assurance requirements and, as a result, its updates were safe and reliable and would not cause

their customers' computers to "blue screen"—i.e., crash. But as CrowdStrike's customers and investors would come to learn, these representations were false, misleading, and omitted material facts. In truth, CrowdStrike and its top executives sought greater profits by prioritizing speed over prudence, shunning the very testing and quality assurance requirements they told investors and customers that they followed. As a result, CrowdStrike issued a faulty software update that resulted in the largest IT outage in history, sowing widespread havoc, destroying customers' trust and erasing billions of dollars of shareholder value.

2. Before releasing software updates to customers, software companies, especially those that make cybersecurity software like CrowdStrike, must adhere to well-established industry standards and federal government requirements relating to testing, quality assurance, and security. They must (i) test their software updates on a computer in a pre-production environment before its release to ensure it works and does not crash customers' computer systems; (ii) roll out the software update in phases to prevent a mass IT outage if their testing fails to catch an error; and (iii) employ a quality assurance team that follows a test plan to execute the testing and roll out of updates. Throughout the Class Period, Defendants led customers and investors to believe that CrowdStrike adhered to these basic, industry-standard requirements before releasing their Falcon software updates to their millions of customers' computers.

3. The Class Period begins on September 20, 2022. On that date, Defendant Kurtz assured investors that, at CrowdStrike, ***"testing and validation is really important"*** and ***"we test more than anyone else, more than all of our next-gen competitors, more than other players that are out there."*** Defendant Kurtz professed to know, first-hand, the importance of this testing. Indeed, prior to their time at CrowdStrike, Defendants Kurtz and Sentonas were Chief Technology Officers of McAfee, another cybersecurity company. While on their watch, McAfee released a

flawed software update that McAfee failed to test in a pre-production environment, which led to a massive IT outage that crippled the company. To assuage any concern that Kurtz and Sentonas might again prioritize short-term profits over customer safety by skipping basic, industry-standard quality assurance and testing processes, Kurtz vowed to CrowdStrike investors that he had ***"learned this lesson at ... McAfee"*** and understood the devastating consequences of customers needing to ***"reboot 300,000 endpoints."***

4. Throughout the remainder of the Class Period, Kurtz and Sentonas stressed time and again, in multiple forums, that they adhered to industry-standard software development requirements and, as a result, CrowdStrike's software updates were safe, stable and would not result in "blue screens"—i.e., crashes. They emphasized that CrowdStrike ***"doesn't blue screen endpoints with failed updates,"*** which was ***"one of the most important things"*** to customers choosing between competing cybersecurity products. They reiterated that CrowdStrike's testing regimen enabled it to ensure that their ***"code is secure, that it's deployed and that it's run in a secure environment"*** prior to any update release to customers. To that end, they represented that CrowdStrike ***"always"*** conducted phased rollouts of their software updates and did ***not*** release their software updates simultaneously ***"to the entire fleet."*** They also touted CrowdStrike's ***"quality assurance team,"*** which was supposedly ***"trained and equipped to assist with testing."***

5. Defendants buttressed their assurances with further representations that CrowdStrike was "meeting the stringent" software development requirements of the federal government, including the Federal Risk and Authorization Management Program ("FedRAMP") and the Department of Defense Cloud SRG Requirements ("DoD"), both of which incorporate the industry standards for information technology and cybersecurity set by the National Institute of Standards and Technology ("NIST"). FedRAMP and DoD specifically require software

companies dealing with the U.S. government, such as CrowdStrike, to test their software updates in a pre-production environment that ***"mirror[s] the configurations in the operational environment … so that the results of the testing are representative of the proposed changes to the operational systems."*** Indeed, before widely deploying a software update, a straightforward way to determine if the update will crash customer computers is to install a test update on an actual computer and monitor its performance to see if any crashes or other issues occur. Such basic testing helps to isolate and fix issues without negatively impacting customer computers. FedRAMP and DoD further require that software companies employ a dedicated quality assurance team to prepare "test plans" as part of their "documented development process," as well as roll out their software updates in a phased process to "determine if [they] should be made widely available" and to prevent a massive IT outage if their update fails. Executives of software companies, like CrowdStrike, seeking FedRAMP or DoD authorization are required to attest that they adhere to each of these requirements in signed declarations before such authorization can be granted.

6. Through Defendants' representations about CrowdStrike's robust testing and quality assurance processes, CrowdStrike amassed a customer base that included the U.S. federal government, 43 out of 50 state governments, and more than half of the Fortune 500 companies. Securities analysts specifically pointed to CrowdStrike's representations about its stable and secure software updates as a reason to recommend that investors "BUY" CrowdStrike's stock. The Company's stock price soared as a result, more than doubling from $174 per share at the beginning of the Class Period to a Class Period high of $392 per share.

7. Unknown to CrowdStrike's investors at the time, however, Defendants' representations were false, misleading, and omitted material facts. A multitude of former CrowdStrike employees have recounted that the Company ***did not*** test its software updates in a

pre-production environment, in contravention of basic industry standards. Defendants' failure meant that CrowdStrike was ***not testing*** on any actual computers whether their updates would cause customers' systems to crash. Nor did CrowdStrike have the necessary test plans or dedicated quality assurance team to properly conduct such tests during the Class Period. As CrowdStrike's former employees reported, ***there were no test plans*** and ***no quality assurance team*** at CrowdStrike during the Class Period.

8. CrowdStrike's former employees have further explained that despite Defendants' representations, Defendants Kurtz and Sentonas sought short-term profits by prioritizing speed above all else, exposing the Company's customers and investors to the risk that CrowdStrike could release a faulty software update, causing a global IT meltdown. Former employees reported that, at CrowdStrike, "quality control was ***not*** really part of our process or our conversation," adding that they "complained about rushed deadlines, excessive workloads, and increasing technical problems to higher-ups ***for more than a year*** before the catastrophic failure of its software."

9. CrowdStrike's investors and customers began to learn the truth on Friday, July 19, 2024. On that day, Defendants pushed out a faulty software update that was ***not*** tested in a pre-production environment, ***not*** reviewed by any quality assurance team, and ***not*** released through a phased rollout. Once released, Defendants' faulty update caused ***every one*** of their customers' 8.5 million Windows machines to simultaneously and immediately "blue screen," taking each of these machines out of commission. The outage caused global disruption, with airlines, public hospitals, financial services, and police departments brought to a complete standstill. In total, insurance experts estimate that the outage caused CrowdStrike's clientele over $5.4 billion in losses due to downtime, increased operational expenses, and remediation costs.

10. Public outrage has been extreme—and justifiably so. Industry experts explained that this was the ***"largest IT outage in history"*** and revealed ***"serious process design failures [in CrowdStrike's] product Quality Assurance."*** They were ***"astounded"*** that CrowdStrike would take such ***"unconscionable"*** risks with the safety and stability of customer systems. Experts stressed, and CrowdStrike did not dispute, that "if [CrowdStrike] ***had just checked*** that this update had run on ***one machine*** successfully ***one time*** before sending it out, ***this would not have happened***." Experts uniformly chided CrowdStrike for its failure to abide by these most basic industry standards, rightfully calling their failure ***"egregious."***

11. Ultimately, Defendants Kurtz and Sentonas "apologized" to their customers and investors. They publicly admitted that ***"we failed you"*** and acted ***"horribly wrong."*** They also acknowledged that CrowdStrike failed to adhere to the basic industry-standard requirements that they long assured investors and customers they scrupulously followed: they admitted that CrowdStrike failed to test its updates on a computer in a pre-production environment and failed to conduct a phased roll-out—revelations that left industry experts ***"slack jawed in horror."*** Defendants vowed to reform, assuring investors that they would ***now*** conduct the testing and quality assurance procedures they represented they always had, leaving industry experts to scoff that Defendants Kurtz, Sentonas, and CrowdStrike "are going to change the design to be what it should have been ***in the first place***."

12. Defendants' professed "apologies" have not erased the tremendous harm that Defendants' misrepresentations and omissions caused investors. The revelations about CrowdStrike's deficient testing and its ramifications caused CrowdStrike's stock price to plummet by nearly ***32%***—the largest stock price decline in CrowdStrike's history as a publicly traded

company. As analysts noted, "[s]hares of CrowdStrike went over a cliff after it became clear that the company was to blame."

13. Defendants' failure to adhere to basic industry standards was so egregious that members of the Congressional Committee on Homeland Security called on Defendant Kurtz to testify, explaining that "Americans will undoubtedly feel the lasting, real-world consequences of this incident" and "deserve to know in detail how this incident happened and the mitigation steps CrowdStrike is taking." And Delta Air Lines, Inc. ("Delta")—one of CrowdStrike's major customers—has now brought a lawsuit against CrowdStrike for its "deceptive and unfair business practices." In its lawsuit, Delta detailed how "CrowdStrike touted compliance with operating system requirements, while altering previously certified computer programming with uncertified and untested shortcuts that damaged and impaired its clients' systems and businesses." Delta stressed that "CrowdStrike ***never*** disclosed that it deployed computer programming and data that circumvented certifications, verifications, and testing, and Delta ***never*** gave CrowdStrike such permission." As Delta explained, "CrowdStrike caused a global catastrophe because it ***cut corners, took shortcuts, and circumvented the very testing and certification processes it advertised, for its own benefit and profit***."

II. JURISDICTION AND VENUE

14. The claims alleged herein arise under Sections 10(b) and 20(a) of the Exchange Act. This Court has jurisdiction over the subject matter of this action pursuant to Section 27 of the Exchange Act and 28 U.S.C. § 1331. Venue is proper in this District pursuant to Section 27 of the Exchange Act and 28 U.S.C. § 1391(b). CrowdStrike maintains its headquarters in Austin, Texas, which is situated in this District, conducts substantial business in this District, and many of the acts and conduct that constitute the violations of law complained of herein, including dissemination to the public of materially false and misleading information, occurred in and/or were

issued from this District. In connection with the acts alleged in this Complaint, Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce, including, but not limited to, the mails, interstate telephone communications, and the facilities of the national securities markets.

III. PARTIES

15. Lead Plaintiff provides financial benefits to state and local public employees, retirees, and their beneficiaries. As reflected in its PSLRA certification filed with the Court herewith, New York State Common Retirement Fund purchased common stock of CrowdStrike at artificially inflated prices during the Class Period and suffered damages as a result of the violations of the federal securities laws alleged herein.

16. CrowdStrike is a company that purports to make its customers' computers safe and secure with its Falcon cybersecurity platform. It is incorporated under the laws of the state of Delaware, with its corporate headquarters and principal place of business in Austin, Texas. CrowdStrike's common stock trades on the NASDAQ under the ticker symbol "CRWD." As of July 30, 2024, CrowdStrike had over 240 million shares of common stock outstanding, owned by many thousands of investors.

17. Defendant Kurtz is the founder and Chief Executive Officer ("CEO") of CrowdStrike. Prior to joining CrowdStrike, he was the global Chief Technology Officer at McAfee. Defendant Kurtz was CrowdStrike's primary spokesperson to investors during the Class Period, including during calls with investors and securities analysts, and also communicated to investors and customers alike by way of the Company's website. As detailed herein, Defendant Kurtz made a series of statements to investors about CrowdStrike's testing and quality assurance controls for its software updates that were false, misleading, and omitted material facts.

18. Defendant Sentonas is the President of CrowdStrike and, before that, was Chief Technology Officer from February 2020 to March 2023. Prior to joining CrowdStrike, he was the Chief Technology Officer-Security Connected and Chief Technology and Strategy Officer, Asia Pacific at McAfee. Along with Defendant Kurtz, Defendant Sentonas regularly spoke to investors on behalf of CrowdStrike during the Class Period, including during calls with investors and securities analysts, and also communicated to investors and customers alike by way of the Company's website. As detailed herein, Defendant Sentonas made a series of statements to investors about CrowdStrike's testing and quality assurance controls for its software updates that were false, misleading, and omitted material facts.

19. Defendants Kurtz and Sentonas directly participated in the management of CrowdStrike's operations, had direct and supervisory involvement in CrowdStrike's day-to-day operations, and had the ability to control and did control the Company's statements to investors, including on CrowdStrike's website. Defendants Kurtz and Sentonas were involved in drafting, reviewing, approving, publishing, and making the Company's public statements, including the false and misleading statements and omissions alleged herein.

IV. SUMMARY OF THE FRAUD

A. CrowdStrike's Purported Compliance With Industry Standards And Federal Requirements Concerning Quality Assurance For Software Updates

20. CrowdStrike is a cybersecurity company that sells software that purports to make its customers' computers safe and secure through reliable and continuous updates. The Company was founded in 2011 by Defendant Kurtz. In June 2013, Defendants Kurtz and CrowdStrike launched their first product—the Falcon cybersecurity platform, which remains CrowdStrike's flagship offering.

21. CrowdStrike dubbed Falcon the first "cloud native, intelligent security solution capable of protecting workloads across on-premise, virtualized, and cloud-based environments running on a variety of endpoints such as laptops, desktops, servers, virtual machines, and IoT devices."[1] Unlike "legacy" products, Falcon was installed through the "cloud," without any "on-premise" (i.e., onsite) installation. Also unlike "legacy" products, CrowdStrike's "updates" to the Falcon software were "automatic" and done through the "cloud," without "requiring [customers] to reboot endpoints or manage updates."[2]

22. Falcon's automatic "updates" were a centerpiece of its value proposition to both customers and investors. According to CrowdStrike, the Falcon platform was uniquely suited to protect its customers because CrowdStrike issued regular, automatic "updates" that incorporated real-time data into the Falcon platform that helped secure its customers' computers.

23. CrowdStrike called this remote update system "Rapid Response." The Rapid Response updates were central to CrowdStrike's investment thesis, as CrowdStrike claimed that its Rapid Response system made its Falcon cybersecurity threat detection software better than its competitors. CrowdStrike emphasized that the Rapid Response updates were "reliable" and "secure," with the Company telling customers and investors alike that its "software development methodology that allows for rapid, frequent, and reliable code updates" and replaces "manual, legacy methods of deploying code to ensure faster and more secure updates."[3]

---

[1] CrowdStrike Prospectus Supplement (Jan. 13, 2021).

[2] Mitesh Shah, *The Security Compromise that Comes with Windows 10 End of Support*, CrowdStrike Blog, https://www.crowdstrike.com/en-us/blog/security-compromise-that-comes-with-windows-10-end-of-support/.

[3] *What is CI/CD?: Pipeline Benefits and Tools*, CrowdStrike, https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/continuous-integration-continuous-delivery-ci-cd/.

1. Basic Quality Assurance Processes Are Critical To Companies Like CrowdStrike That Remotely Update Customer Software

24. The software industry has long identified certain basic controls that are necessary when designing, testing, and deploying remote, cloud-based software updates to customers. These controls are important: while software updates are designed to keep computers operating correctly, "without due diligence, the reverse can happen"—i.e., a software update can crash a computer system.[4] A software developer updating customer software could, absent necessary controls in the software development process, introduce coding errors to millions of devices "resulting in sensor malfunction, data loss, crashes, and breaking key device functionality."[5] As industry experts have cautioned, if software companies fail to follow industry-standard requirements, "automatic software updates pose a greater risk than malware."[6]

25. Defendants publicly recognized the importance of quality assurance and secure and stable software updates. For example, while representing CrowdStrike in testimony before the U.S. Senate Select Committee on Intelligence prior to the Class Period, Defendant Kurtz emphasized the need for industry and government actors to practice "secure software development," adding that "organizations ***must*** incorporate secure implementation of both hardware and software, conduct architecture reviews, deploy code signing via tamper resistant hardware, engage in ongoing monitoring, and regular testing."[7]

---

[4] Anthony Wall, *Beyond the Download: Resetting the Vulnerabilities of OTA Updates*, Electronic Design, https://www.electronicdesign.com/technologies/embedded/article/55091113/beyond-the-download-resetting-the-vulnerabilities-of-ota-updates.

[5] *Id.*

[6] Theo - t3.gg, *Diving into the embarrassing engineering behind CrowdStrike,* YouTube (July 25, 2024), https://www.youtube.com/watch?v=7rx4U5TlaqE.

[7] George Kurtz's Testimony on Cybersecurity and Supply Chain Threats to the Senate Select Committee on Intelligence (Feb. 23, 2021), https://www.crowdstrike.com/wp-content/uploads/2021/03/george-kurtz-senate-testimony-on-cybersecurity-and-supply-chain-threats-022321.pdf.

26. Basic controls are even more critical for software like Falcon because, to function as designed, Falcon software requires an unusually high level of access to customers' computer systems. Most software operates at the "user level," meaning that such software cannot directly control the computer's operating system (i.e., Microsoft Windows) or system hardware (i.e., a physical computer). User-level software can only impact the operation of a computer by obtaining permissions to do so from the operating system. Software generally operates at the user level whenever possible because it presents less risk to the computer than software that accesses the computer's operating system or hardware.

27. CrowdStrike's Falcon software, however, operated at the "kernel level," rather than the "user level." The kernel is the heart of a computer's operating system and is responsible for controlling and managing hardware resources, processes, and memory.[8] Unlike user-level software, a program that runs in the kernel operates as part of the operating system, and thus controls the operating system and computer hardware without any intermediary. Kernel-level software has vastly greater permissions and access to the operation of the computers on which it is installed.

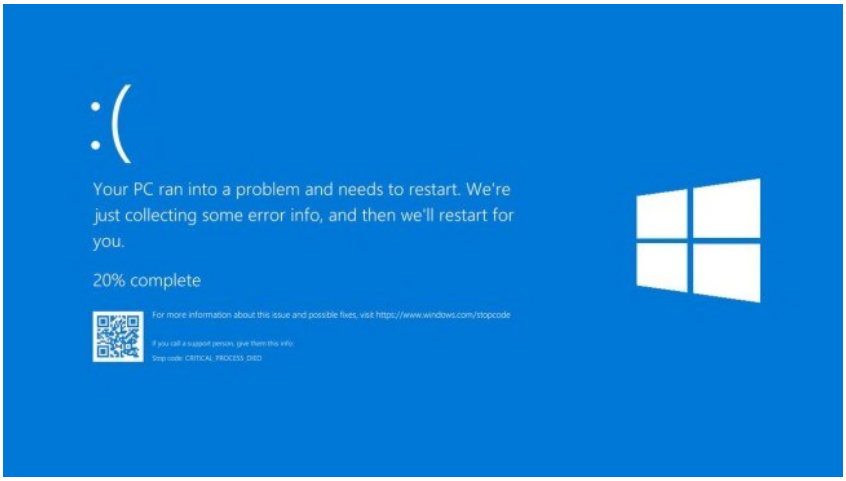
28. Defendant Kurtz told investors that the fact that Falcon runs in the kernel gave CrowdStrike a "clear advantage" over its competitors by providing CrowdStrike unfettered access to its customers' entire computer systems.[9] But with that competitive edge came heightened risk

[8] Anthony Harrison, *CrowdStrike and kernel-level access: a deep dive*, BCS: The Chartered Institute for IT (Oct. 20, 2024), https://www.bcs.org/articles-opinion-and-research/crowdstrike-and-kernel-level-access-a-deep-dive/.

[9] Sept. 20, 2022 CrowdStrike Holdings, Inc. Presents at CrowdStrike Fal.con 2022 transcript at 4.

and increased responsibility. This was well-known to Defendants, with industry participants "aware of the stakes when you run code in the kernel."[10]

29. Because of the near-limitless access a kernel driver has to monitor and control a computer's operating system, a coding error introduced in kernel-level software can have catastrophic consequences, particularly as compared to the lower risks associated with user-level software. If a coding error is introduced to user-level software, this may cause a single program to crash, but should have a limited effect, if any, on the computer's overall operating system or hardware. But if a coding error is introduced to kernel-level software, that same coding error has the potential to crash the entire operating system, resulting in the following Windows "blue screen" error message:



30. Once a bug or coding error is introduced to the kernel, the operating system has no choice but to go into a blue screen. A blue screen means that the user's computer has become inoperable. It requires, at the very least, a restart of the user's computer and may require a physical reset or other fix, risking the loss of work product that was unsaved at the time of the crash. In some cases, referred to as a "blue screen loop," re-starting the computer will not remedy the issue,

[10] Dave's Garage, *CrowdStrike IT Outage Explained by a Windows Developer*, https://www.youtube.com/watch?v=wAzEJxOo1ts.

but rather will bring the user back to the blue screen and prevent the computer from re-starting altogether.

31. For companies that rely on hundreds or thousands of computers to keep their businesses moving, a widespread blue screen crash is catastrophic. For example, major airlines rely on tens of thousands of computers to handle everything from ticket sales, air traffic management, baggage tracking, customer service, and more. If such airlines experience a widespread blue screen crash, the airlines will have to, if it is even possible, manually perform all of those tasks, if not ground flights altogether, until an IT specialist institutes a fix that is hopefully able to reset every single computer. In the event that restarting the computers begins a blue screen loop, the computers will remain unusable, causing even more lost operational time and potential revenues.

32. CrowdStrike understood that its customers expected it to ensure that its software updates would not crash critical computer systems or necessitate reboots. As Defendant Kurtz explained on calls with investors, "[A] lot of people don't realize how hard it is for big companies to keep up to date" when "[t]hey have to reboot their systems and there's operational impact."[11] And Defendant Kurtz specifically told investors that CrowdStrike was winning business precisely because customers had "experience[ed] several outages caused by sensor updates" with competitors' software in the past.[12]

33. For these reasons, industry participants have long understood that certain basic quality assurance processes for the development of software updates are necessary to prevent blue screens, including: (i) testing the software update on a computer before its customer release to

[11] Oct. 12, 2021 Investor Meeting transcript at 9.
[12] June 3, 2021 Q1 2022 Earnings Call transcript.

ensure the update works and does not crash computers in the real world; (ii) rolling out the software update in phases to prevent a mass IT outage if the testing failed to catch an error; and (iii) employing a quality assurance team that follows a test plan to execute the testing, and roll-out of the software update. These basic requirements are further discussed below.

34. ***Testing in a pre-production environment.*** To prevent outages from coding errors in software updates, it is essential and standard in the industry for software updates to be tested in a "pre-production environment." A "pre-production environment" (also known as a "staging environment") is a testing environment that must "nearly mirror what the end users would see in the production environment."[13] Prior to implementing an update, software companies must test the update in an environment where the "features' functionality is very similar to what [the] actual user experiences on the live system."[14] Such basic testing is necessary to ensure that the software "is developed per specifications and works without any critical or significant bugs that can harm the users."[15] For example, if a developer has built an update to software that runs on Microsoft Windows, the developer must load that update onto a computer running Microsoft Windows to test how the system functions with the update implemented before deploying the update. To the extent that such an update causes the computer system to crash or fail to boot, testing on a machine in a pre-production environment will immediately reveal such issues. As industry experts have explained, it is "essential" to conduct "rigorous testing in staging environments before moving to production," as "testing solely within a controlled development environment overlooks the

[13] *What is a Pre-Production Environment*, https://www.pagerduty.com/resources/learn/what-is-production-environment/.
[14] David Berclaz, *What Test Environments do you need? Dev, Test, Staging?*, https://www.apwide.com/what-test-environment-dev-test-staging-preprod/.
[15] *Id.*

intricacies and configurations found in production, particularly for cloud-native applications that must operate within dynamic, interconnected systems."[16]

35. Defendants themselves have acknowledged the basic requirement to test in a pre-production environment, stating on the CrowdStrike website that software updates should be—and, at CrowdStrike, purportedly were—pushed out to users only "[i]f the code passes all tests, the artifacts are deployed to a staging environment that closely resembles the production environment" and if the update underwent "[p]erformance testing, security testing, user acceptance testing (UAT), and other testing."[17] Defendants further publicly recognized the need to "deploy[] code changes to a pre-production environment," in order to ensure that the software update is appropriately tested before being released to its customers.[18]

36. Defendant Kurtz also repeatedly emphasized the importance of testing in a pre-production environment in a book he wrote prior to the Class Period titled *Hacking Exposed*. In his book, Defendant Kurtz acknowledged that software developers conducting "rapid patch deployment" must "be sure to test new patches for compatibility with the environment and applications."[19] Defendant Kurtz specifically recognized in his book that ***"as always, you should try your changes in a test environment"*** before deploying to the production environment. As

---

[16] *See* Shira Shamban, *What the CrowdStrike outage teaches us about cloud security*, https://www.scworld.com/perspective/what-the-crowdstrike-outage-teaches-us-about-cloud-security. Shira Shambam is co-founder and CEO at Solvo, a software company focused on automating cloud and data security. Ms. Shambam specializes in cloud security and is lecturer and mentor for organizations such as SheCodes, Cyber Ladies, and Women in AppSec. *See* Shira Shamban, LinkedIn, https://www.linkedin.com/in/shira-shamban/.

[17] *What is CI/CD?: Pipeline Benefits and Tools*, CrowdStrike.com, https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/continuous-integration-continuous-delivery-ci-cd/.

[18] *Id.*

[19] Stuart McClure, Joel Scambray, George Kurtz, Hacking Exposed 7 (ed. 7) (July 10, 2012) at 293.

Defendant Kurtz has also emphasized to investors, such testing is essential: one needs to "make sure that you're not putting tainted containers and vulnerabilities into your pipeline."[20]

37. The basic requirement to test software updates in a pre-production environment has been specifically recognized by the NIST, which (as Defendants have publicly acknowledged) is the "industry standard" for software companies like CrowdStrike.[21] In particular, the NIST requires that software companies test updates in an "environment" that "mirror[s] the configurations in the operational environment … so that the results of the testing are representative of the proposed changes to the operational systems."[22] Such testing must "occur[] at ***all*** post-design phases of the system development life cycle … to ensure that activities in the test environment do not impact activities in the operational environment."[23]

38. ***Quality Assurance Team and Test Plans.*** To ensure that software updates are properly tested and deployed to customers safely, it is also a basic industry standard that software companies maintain a dedicated quality assurance team. Industry experts have long explained that dedicated quality assurance teams are a necessary and important aspect of software development.[24] A dedicated quality assurance team at a software company ensures that insecure, unstable, and faulty code is "address[ed] early in the development cycle," so that "the development team can

[20] Dec. 8, 2022 CrowdStrike Holdings, Inc. Presents at Barclays 2022 Global Technology, Media and Telecommunications Conference transcript.
[21] CrowdStrike, *Frictionless Zero Trust,* CrowdStrike.com (2022), crowdstrike-frictionless-zero-trust-verify-infographic.pdf
[22] FedRAMP Security Controls Baseline, at CM-2 (6), https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Controls_Baseline.xlsx.
[23] *Id.* at CM-04 (01).
[24] *Fintech: Rooted in the Past, Borrowed from the Future,* https://cisomag.com/fintech-rooted-past-borrowed-future/.

resolve them before they escalate."[25] "Unlike ad-hoc testing by developers or other departments, a dedicated team focuses exclusively on quality, ensuring thorough testing coverage."[26] Quality assurance teams conduct the necessary tests of software updates and ensure that they do not crash customers' computers upon release.

39. One of the main functions of a dedicated quality assurance team is to create "test plans" for testing software updates. A test plan operates "as a roadmap for the entire software project testing process" and details "the resources, timelines, and responsibilities associated with the testing activities."[27] A test plan provides a structured approach to testing, making certain that all aspects of the software are thoroughly tested to identify and address any potential issues. As the DoD has explained, software companies like CrowdStrike must create and follow a "test plan," with "all tests start[ing] with test planning and test development, which includes detailed test procedures."[28]

40. The NIST also recognizes the need for companies, like CrowdStrike, to maintain dedicated quality assurance staff to conduct testing of software updates. Specifically, the NIST requires software companies to "conduct[] information system support functions with different individuals," including "quality assurance and testing," and make certain that "personnel administering access control functions do not also administer audit functions."[29] The NIST

---

[25] Pradeep K, *5 Reasons Why Your Business Needs a Dedicated Testing Team*, TestVox, https://testvox.com/5-reasons-why-your-business-needs-a-dedicated-testing-team/.
[26] *Id.*
[27] *Penetration Testing Plans v. Test Cases*, https://bluegoatcyber.com/blog/whats-the-difference-between-test-plan-and-test-case/.
[28] DevSecOps Fundamentals Guidebook: DevSecOps Tools & Activities, U.S. Dept. of Defense (Mar. 2021), at 22, https://dodcio.defense.gov/Portals/0/Documents/Library/DevSecOpsTools-ActivitiesGuidebook.pdf.
[29] *Security and Privacy Controls for Federal Information Systems and Organizations*, National Institute of Standards and Technology (U.S. Dept. of Commerce) (Sept. 23, 2021) at AC-5, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

emphasizes the importance of this "separation of duties," requiring that different individuals are responsible for "system management, programming, configuration management, quality assurance and testing, and network security."[30] The NIST further requires that software companies create and adhere to test plans for software updates, explaining that software companies must "follow a documented development process" that, among other things, "explicitly addresses security requirements, identifies the standards and tools used in the development process … and ensures the integrity of changes."[31]

41. ***Phased Rollouts.*** To make certain that software updates do not cause a mass IT outage, it is also a basic requirement for software companies to conduct "phased" rollouts of any new updates. Phased rollouts, which are also referred to in the industry as "canary" rollouts, are an essential step with any software update, requiring the "gradual implementation of a new feature to a smaller cohort of users at one time rather than all users at once."[32] As cybersecurity expert Shira Shamban has explained, "companies should roll out updates to a small segment of users first, monitor[] the impact closely, and only expand[] the release if no issues arise."[33] Cybersecurity expert James Smith has likewise explained that, with phased rollouts, "engineering teams catch issues early in the process so they can quickly fix them and resume the rollout of the experiment, which prevents issues from impacting millions of users down the road."[34] Software developer

[30] *Id.*
[31] *Id*. at SA-15.
[32] James Smith, *Do's and Don'ts of Phased Rollouts Software Delivery*, DevOps (Sept. 9, 2021), https://devops.com/dos-and-donts-of-phased-rollouts-software-delivery/.
[33] *See* Shira Shamban, *What the CrowdStrike outage teaches us about cloud security*, SC Media, https://www.scworld.com/perspective/what-the-crowdstrike-outage-teaches-us-about-cloud-security.
[34] James Smith is the founder of the software security management company Bugsnag. James Smith, *Do's and Don'ts of Phased Rollouts Software Delivery*, DevOps (Sept. 9, 2021), https://devops.com/dos-and-donts-of-phased-rollouts-software-delivery/.

Rajiv Kottomtharayil added, "By exposing the change to a limited group, potential problems can be identified and addressed before they impact a larger audience."[35] Industry expert Talal Haj Bakry likewise explained that for software running on millions of computers and in the kernel, like the Falcon platform, "every change—no matter how small it may seem" must be subject to phased rollouts.[36] And cybersecurity expert Alex Stamos has confirmed that, when SentinelOne (a competitor of CrowdStrike) issues any software update, it rolls it out to "small percentages of customers" to confirm that the update operates as intended—which is a "super basic" requirement in the industry that "anyone who has ever done high-quality engineering has done for decades."[37] CrowdStrike similarly recognized the importance of a phased deployment strategy, publicly stating that "[f]or system stability, we ***always*** do canary deployments of new services before rolling out changes to the entire fleet."[38]

42. The DoD requires compliance with the industry standard that software companies, such as CrowdStrike, conduct phased rollouts for software updates. Specifically, the DoD requires

---

[35] Rajiv Kottomtharayil is the vice president of product development at Commvault, Mr. Kottomtharayil received his Master of Science degree in Computer Science from Monmouth University and Bachelor of Science degree in Electronics from Bombay University. *See* Rajiv Kottomtharayil, *The CrowdStrike Incident: A Cautionary Tale for Software Releases*, Commvault (Aug. 12, 2024), https://www.commvault.com/blogs/the-crowdstrike-incident-a-cautionary-tale-for-software-releases.

[36] Talal Haj Bakry is a cybersecurity expert and researcher at Mysk. *See* Kate O'Flaherty, *CrowdStrike Reveals New Details About What Caused Windows Outage*, Forbes, https://www.forbes.com/sites/kateoflahertyuk/2024/07/24/crowdstrike-reveals-new-details-about-what-caused-windows-outage/.

[37] Risky Business Media, *Why CrowdStrike's Baffling BSOD Disaster Was Avoidable*, https://www.youtube.com/watch?app=desktop&v=EGRqtscp4eE; Alex Stamos is a cybersecurity expert and entrepreneur. Mr. Stamos is an Adjunct Professor and Lecturer in Computer Science at Stanford University and the Chief Information Security Officer at SentinelOne, a cybersecurity company. Mr. Stamos previously served as Chief Information Security Officer at Yahoo! Inc. and Chief Security Officer at Facebook. *See* Alex Stamos, LinkedIn, https://www.linkedin.com/in/alexstamos/.

[38] *Unexpected Adventures in JSON Marshaling*, CrowdStrike.com, https://www.crowdstrike.com/en-us/blog/unexpected-adventures-in-json-marshaling/.

"canary deployments" of software updates to "determine if [the new feature] should be made widely available, or if the feature needs to be re-worked" before a wider release.[39] This means that software companies are required to first deploy new updates to just a subset of customers to monitor for issues that arise during use in the operational environment and, only after such monitoring reveals that the update functions as designed, may the company release the update to its remaining customers.

* * *

43. Before and during the Class Period, Defendants Kurtz and Sentonas knew firsthand how critical testing in pre-production environments and phased rollouts were when releasing software updates to customers. Before joining CrowdStrike, Defendants Kurtz and Sentonas were Chief Technology Officers at McAfee, another company that sold cybersecurity software. While at McAfee, they failed to test a faulty software update in a pre-production environment, and then failed to employ a phased rollout when they released that faulty update to all of its customers. Because of these failures, McAfee's customers experienced blue screens that disrupted their businesses and caused substantial financial losses. The outage caused severe reputational harm to McAfee, ultimately forcing McAfee to sell itself to another tech company at a steep discount.[40] As commentators widely noted, "[T]he root cause [of the McAfee outage] turned out to be a complete breakdown of the QA [quality assurance] process."[41] Commentators further noted at the

[39] *DoD Enterprise DevSecOps Fundamentals*, U.S. Dept. Of Defense (Mar. 2021) at 15, https://dodcio.defense.gov/Portals/0/Documents/Library/DoDEnterpriseDevSecOpsFundamentals.pdf.

[40] Akash Pandey, *McAfee-caused PC meltdown and Microsoft-CrowdStrike outage have a common connection*, NewsBytes, https://www.newsbytesapp.com/news/science/defective-mcafee-once-caused-worldwide-meltdown-of-windows-xp-pcs/story.

[41] Ed Bott, *What caused the great CrowdStrike-Windows meltdown of 2024? History has the answer*, ZDNet, https://www.zdnet.com/article/what-caused-the-great-crowdstrike-windows-meltdown-of-2024-history-has-the-answer/.

time that McAfee could have prevented the crash if it had tested its update in a pre-production environment before pushing it out to customers, describing such a process as "very basic testing, not something weird or intricate" and adding that "[t]he fact that McAfee didn't see this as part of normal testing is really shocking."[42]

2. CrowdStrike Consistently Assured Investors That Its Software Update Process Was Consistent With Industry Standards And Federal Compliance Requirements

44. Throughout the Class Period, Defendants publicly assured customers and investors that CrowdStrike's updates were stable, secure, and would not cause blue screens on their customers' systems on which millions of people and thousands of businesses relied. As discussed further below, Defendants repeatedly represented to investors that they mitigated the risks of their remote updates through robust pre-production testing and a phased rollout, all overseen by a dedicated quality assurance team, in accordance with industry standards and the stringent requirements governing the development of software for the U.S. government.

45. **Defendants touted CrowdStrike's testing of updates.** During the Class Period, Defendants repeatedly emphasized the soundness, stability, and security of CrowdStrike's software updates and its quality assurance processes. They stated to investors that CrowdStrike tested its updates in pre-production environments to ensure that any coding errors were resolved prior to implementation. They had, as Defendant Kurtz told CrowdStrike's investors, ***"learned [their] lesson at ... McAfee,"*** which (as discussed above) failed to test its updates in a pre-production environment prior to release and, after inadvertently releasing a faulty update, required customers "to reboot 300,000 endpoints," an outcome that "[n]o one wants to do."[43]

---

[42] Bryan Acohido, *Massive manual PC cleanup expected after McAfee error*, USA Today (Apr. 22, 2010), http://content.usatoday.com/communities/technologylive/post/2010/04/massive-manual-pc-cleanup-triggered-by-mcafee-error/1.

[43] Mar. 7, 2024 Morgan Stanley Technology, Media & Telecom Conference transcript at 4.

46. Against this backdrop, Defendants specifically and repeatedly highlighted their testing of CrowdStrike's software before its release. For example, on September 20, 2022 (the first day of the Class Period), Defendant Kurtz assured investors that, at CrowdStrike, ***"[t]esting and validation is really important,"*** stressing that ***"[w]e test more than anyone else, more than all of our next-gen competitors, more than other players that are out there."***[44] Again, during an August 30, 2023 CrowdStrike quarterly earnings call, Defendant Kurtz told investors that CrowdStrike's testing ensured that it would identify beforehand and, thus, prevent ***"insecure code … being put into the [update] pipeline."***[45] During another investor conference call a week later, Defendant Kurtz told investors that CrowdStrike had ***"the ability to help make sure that code is secure, that it's deployed and that it's run in a secure environment."***[46] In CrowdStrike's public presentations, they further represented that the Company tests its Falcon software updates ***"in non-production environments" before "roll[ing] them out."***[47]

47. **CrowdStrike further assured investors that Falcon updates would not cause a blue screen**. CrowdStrike's testing practices were crucial to customers that relied on its Falcon software. These testing practices were necessary to ensure that Falcon's updates would not cause their customers' computers to blue screen—i.e., crash.

48. On investor calls, Defendants Sentonas and Kurtz repeatedly assured investors that CrowdStrike's software updates were thoroughly tested before they were released to customers and, thus, would ***not*** result in a blue screen. For example, during an April 4, 2023 investor

[44] Sept. 20, 2022 CrowdStrike Presents at CrowdStrike Fal.con 2022 transcript at 4.
[45] Aug. 30, 2023 CrowdStrike Holdings, Inc., Q2 2024 Earnings Call transcript at 15.
[46] Sept. 5, 2023 CrowdStrike Presents at Goldman Sachs Communacopia & Technology Conference transcript at 10.
[47] EliteCISOs For CISOs by CISOs, *CrowdStrike Session CrowdStrike Powers the SOC of the Future with Next-Gen*, https://www.youtube.com/watch?v=tLlKo2m8fqU.

conference, Defendant Sentonas squarely represented to investors that Falcon software ***"doesn't blue screen endpoints with failed updates,"*** which he stated was ***"one of the most important things"*** to CrowdStrike's customers.[48] Defendant Kurtz likewise told investors during a November 28, 2023 investor earnings call that CrowdStrike was able to sell its software to "many, many airlines" precisely because its updates do ***not*** require such customer "to send out an IT person to go fix a kiosk that has a Microsoft blue screen."[49] Defendant Kurtz made a similar representation just weeks later at another investor conference, during which he told investors that Falcon's updates (unlike its competitors' software) would ***not*** produce "blue screens," emphasizing that "[w]e have airlines that you know when the kiosk is kind of blue screened, you know when you go through the airport and you see the Microsoft blue screen, they actually, yeah well ***they actually use our technology to fix it***."[50]

49. Additionally, Defendants specifically assured investors that, consistent with industry standards, CrowdStrike released its software updates through phased rollouts (also known as "canary" rollouts), through which the impact of any coding errors would be contained and limited to a subset of customers. In this regard, CrowdStrike represented on its website that "[f]or system stability, we ***always*** do canary deployments of new services before rolling out changes to the entire fleet."[51]

50. **Defendants assured investors that CrowdStrike had a "quality assurance team."** Defendants further secured both customer and investor trust by representing that, in

[48] Apr. 4, 2023 CrowdStrike Holdings, Inc. (CRWD) Investor Briefing transcript at 7.
[49] Nov. 28, 2023 Q3 2024 Earnings Call transcript at 16.
[50] The Compound and Friends, *Surprise! A conversation with CrowdStrike CEO George Kurtz*, Podcast (Dec. 29, 2023), https://osmosis.fm/ep/The-Compound-and-Friends-Surprise-A-conversation-with-CrowdStrike-CEO-George-Kurtz.
[51] *Unexpected Adventures in JSON Marshaling*, CrowdStrike.com, https://www.crowdstrike.com/en-us/blog/unexpected-adventures-in-json-marshaling/.

accordance with industry standards, CrowdStrike had a "quality assurance team." A quality assurance team at a software company ensures that unstable or faulty code is "address[ed] early in the development cycle," so "the development team can resolve them before they escalate."[52] "Unlike ad-hoc testing by developers or other departments, a dedicated team focuses exclusively on quality, ensuring thorough testing coverage."[53] In each of CrowdStrike's annual Proxy Statements, Defendants told investors that—consistent with industry standards—they ***had*** a quality assurance team, representing to investors that "[i]n addition to some automated accessibility compliance testing as part of our continuous integration and deployment flow, ***our quality assurance team is also trained and equipped to assist with testing for accessibility***."[54]

51. **CrowdStrike assured investors that it adhered to the requirements of the U.S. government.** To garner additional customer and investor confidence, CrowdStrike also publicly stated that it adhered to the U.S. government's specific requirements for robust testing of software updates overseen by a quality assurance team and in accordance with a detailed test plan. Defendants' representations on this front were important to investors, including because CrowdStrike needed to comply with these standards to win and maintain business from the federal government (one of its largest customers) to support the Company's continued growth.

52. Defendants used their purported compliance with these standards as part of their pitch to both investors and customers. They told them that "meeting these stringent requirements reinforces CrowdStrike's commitment and ability to serve customers of all types."[55] They added

[52] Pradeep K, *5 Reasons Why Your Business Needs a Dedicated Testing Team*, TestVox (Oct. 29, 2024), https://testvox.com/5-reasons-why-your-business-needs-a-dedicated-testing-team/.
[53] *Id.*
[54] CrowdStrike Schedule 14A (May 14, 2021).
[55] *The Federal Risk and Authorization Management Program (FedRAMP) FAQ*, CrowdStrike (Jan. 6, 2024), https://www.crowdstrike.com/en-us/solutions/government-public-sector/federal-

that even non-governmental "[c]ustomers who are not subject to these requirements gain assurance" knowing that CrowdStrike supposedly meets the government's requirements.[56]

53. In particular, Defendants represented that CrowdStrike was "[m]eeting the stringent requirements" of the Federal Risk and Authorization Management Program ("FedRAMP"). As CrowdStrike has acknowledged, "FedRAMP is a crucial component of cloud security frameworks, particularly for cloud service providers seeking to do business with U.S. government agencies."[57] CrowdStrike has further acknowledged that FedRAMP "standardizes how non-government entities implement security controls to ensure they align with government standards for assessment, authorization, and monitoring in the cloud."[58]

54. In addition to FedRAMP, CrowdStrike also specifically represented to investors that it "meet[s] the … compliance requirements" of the U.S. "Department of Defense" (the "DoD"). As CrowdStrike has acknowledged, the DoD "defines security controls and requirements necessary for using cloud-based solutions within the DoD."[59] Defendant Kurtz touted CrowdStrike's purported compliance with the DoD's requirements during investor conferences, telling investors that such compliance "positions us well to extend our reach into the massive defense IT and cybersecurity markets."[60]

---

risk-and-authorization-management-program-fedramp-faq/#accordionfaq-en-us-10-04-2024-item-8.

[56] *Id.*

[57] Sameer Vasanthapuram, *Cloud Security Frameworks: How to Choose the Right One for Your Business*, CrowdStrike Blog (Feb. 19, 2024), https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/cloud-security-frameworks/.

[58] *Id.*

[59] CrowdStrike, *Falcon on GovCloud: Secure Your Public Sector Enterprise with a Solution that Provides Unrivaled Protection and Optimal Scalability*.

[60] May 31, 2023 CrowdStrike Holdings, Inc., Q1 2024 Earnings Call transcript at 5-6.

55. As discussed above and in more detail below (¶¶ 37-42, 106), FedRAMP and DoD expressly mandate that software companies like CrowdStrike: (i) test new updates in a pre-production environment that replicates the production environment such software will run on when released to customers, (ii) utilize a phased rollout process to ensure that errors are identified in a small number of production environments before updates are released to the vast majority of customers, and (iii) maintain quality assurance staff distinct from software developers to conduct such testing and in accordance with standardized test plans. The federal government also requires companies seeking FedRAMP or DoD authorization to explicitly certify that they meet the above requirements. Former Employee ("FE") 8, who was a Distribution Channel Account Manager for the U.S. Public Sector and a Federal Regional Alliance Manager for the DoD/IC at CrowdStrike,[61] stated that Defendant Kurtz or someone else in the C-Suite, including Defendant Sentonas, had to sign certifications to the federal government attesting to CrowdStrike's compliance with FedRAMP and DoD requirements. FE 8 confirmed that such signed certifications would affirm, among other things, that CrowdStrike (i) tested new software or updates in an internal pre-production environment that mimics the conditions associated with the production environment, (ii) released new software or updates to customers using "canary deployment" or "phased rollout" processes, and (iii) maintained a dedicated quality assurance team or staff.

56. Analysts and investors trusted Defendants' representations about CrowdStrike's testing and quality assurance. For example, in a December 21, 2023 report, securities analysts at Needham & Company, LLC wrote, "We think CRWD is one of the best-positioned Security

[61] FE 8 was a Distribution Channel Account Manager – U.S. Public Sector at CrowdStrike from April 2020 to February 2022, then a Federal Regional Alliance Manager - DoD/IC at CrowdStrike from February 2022 to February 2023. In both roles, he reported to Matt Kelly, Director of Public Sector Partnerships.

vendors to benefit from the Federal sectors accelerating investment in Cybersecurity," noting that its purported compliance with FedRAMP and the DoD's requirements put it in "rarified territory vs. other competitors."[62] Likewise, in a December 5, 2023, report, analysts at Scotiabank highlighted CrowdStrike's purported compliance with "FedRamp …, which allows CRWD to sell to the Department of Defense and additional federal agencies" as a reason to buy CrowdStrike's stock.[63]

* * *

57. On the back of CrowdStrike's public representations about its purported testing of its software updates, CrowdStrike became the fastest-growing cybersecurity vendor and amassed over 29,000 subscription customers worldwide,[64] which included major U.S. government agencies and contractors, some of the world's largest tech companies (such as Amazon, Google, and Intel), critical infrastructure providers (such as Delta and United Airlines), and other large business and organizations (such as Target Corporation and the AARP).

58. CrowdStrike's stock price skyrocketed as a result. Indeed, the price of CrowdStrike stock ***more than doubled*** during the Class Period. In the first half of 2024 alone, the price of CrowdStrike's stock increased by over ***150%***, with popular television analyst Jim Cramer of *CNBC*'s Mad Money telling his viewers that CrowdStrike stock was a "Cramer Favorite."[65] At its

[62] Dec. 21, 2023 Needham & Company, LLC analyst report at 6, *Top Pick in Security, CRWD Positioned to Deliver Again in '24*.
[63] Dec. 5, 2023 Scotiabank analyst report, *Fireside Chat Takeaways – Global Technology Conference*.
[64] CrowdStrike 10-K for the fiscal year ended January 31, 2024 (Mar. 7, 2024).
[65] Bradley Guichard, *CrowdStrike's Stock Price Just Exploded. Time to Buy?*, The Motley Fool (June 13, 2024), https://www.fool.com/investing/2024/06/13/crowdstrikes-stock-price-just-exploded-time-to-buy/; NBC Television, *CrowdStrike CEO George Kurtz goes one-on-one with Jim Cramer*, YouTube (June 5, 2024), https://www.youtube.com/watch?v=X4ZOqQHkbXU.

Class Period peak, just days before the stunning truth was revealed about CrowdStrike's actual practices, the Company's stock reached an all-time high of $392 per share.

B. Unknown To Investors, CrowdStrike Failed To Conduct Necessary Tests Of Software Updates, Roll Out Updates In Phased Releases, And Otherwise Comply With Industry Standards And The Government's Requirements

59. Defendants' statements touting CrowdStrike's robust testing and compliance with government requirements and industry standards were false, misleading, and omitted material facts. Unknown to investors during the Class Period, CrowdStrike's testing of software updates and quality assurance practices were severely deficient. In particular, CrowdStrike (i) failed to test its software updates in a pre-production environment before pushing them out to customers; (ii) lacked a quality assurance team or even test plans for its software updates; and (iii) released updates to all customers at the same time, instead of conducting phased rollouts. Defendants knew or were, at minimum, severely reckless in not knowing these facts concealed from investors.

60. **First**, CrowdStrike failed to conduct pre-production environment testing on its Falcon software updates prior to their release to customers. As discussed above (¶¶ 44-55), Defendants led investors to believe throughout the Class Period that CrowdStrike tested its software updates in a pre-production environment prior to pushing those updates out to customers. Lead Counsel's extensive investigation, which included, among other things, speaking with former CrowdStrike employees, demonstrates that CrowdStrike's testing procedures were not as represented and deficient, with Defendants prioritizing the speed of its update releases over testing to maximize profits.

61. Numerous former CrowdStrike employees responsible for developing CrowdStrike's software and its updates, as well as teams responsible for managing projects at CrowdStrike, confirmed that CrowdStrike did not conduct necessary tests of Falcon updates before rolling them out to customers, and were instructed to prioritize speed above all else in the pursuit

of short-term profits.[66] Because of CrowdStrike's prioritization of speed over stability of software development, CrowdStrike did not conduct testing of Rapid Response updates in pre-production environments prior to their release.

62. FE 1, a Senior Technical Operations Engineer on the forensics team from November 2022 to October 2023, explained that CrowdStrike was not testing whether such updates would affect a Microsoft Windows machine's boot process.[67] FE 1 explained that to know whether a software update would cause issues on a customer's computer that would affect the computer's ability to boot (i.e., start), CrowdStrike would need to test such update on a computer running Microsoft Windows. But, in FE 1's experience, CrowdStrike did ***not*** do this testing. FE 1 added that, in his experience as a test engineer for over ten years, CrowdStrike's failure to conduct such testing stood out to him while he was at the Company.

63. FE 2, a Senior Network Engineer at CrowdStrike from January 2018 through November 2024, also confirmed that, if CrowdStrike had tested its software updates in a pre-production environment, it would have found the faulty update that caused the IT outage. FE 2 explained that CrowdStrike's software update was not tested because if it had been tested in an isolated, pre-production environment that mimicked the production environment as the customers view it, the issue definitely would have shown up before it was released to CrowdStrike's customers.[68] FE 2 reiterated that new code and definition files need to be tested with equal

[66] In order to preserve the anonymity of former employees who provided reports for this Complaint, "he/him/his" pronouns are used throughout.

[67] FE 1 was a Senior Technical Operations Engineer on the forensics team from November 2022 to October 2023. FE 1 reported directly to a team lead manager, Lakshmi Kiran, and her manager was John Stuart. FE 1 was responsible for testing of the forensic system for Falcon.

[68] FE 2 worked at CrowdStrike from January 2018 until November 2024 as a Senior Network Engineer in their IT department. As such, he managed the internal networking and security wireless infrastructure for the Company.

intensity, and it is standard practice to utilize the same testing protocols, including testing in a pre-production environment, regardless of whether the update in question was new code or a definition file. FE 2 added that other network companies he had worked at prior to CrowdStrike would not roll a code out to customers without testing it first to verify it is not breaking anything. FE 2 noted that, after the CrowdStrike IT outage, he was instructed by CrowdStrike's IT Director, Chris Kiffe, to set up a lab with twenty Microsoft Windows laptops on which to conduct such testing, and that he did not believe any such testing lab to have existed prior.

64. CrowdStrike's failure to conduct necessary tests was long-standing. Jeff Gardner, a former CrowdStrike Senior User Experience Designer who worked at the Company from April 2021 until December 2022, explained that, in his role, he worked with CrowdStrike's engineering team to design software, and engineers used designs from Gardner's team as a reference point for actually building the software.[69] Mr. Gardner explained that, at CrowdStrike, there was a ***"complete lack of QA process,"*** with a ***"'wild west' code check in and rolling processes."*** Mr. Gardner added that, at CrowdStrike, ***"quality control was not really part of our process or our conversation."*** Mr. Gardner further explained that ***"CrowdStrike as a leadership had not established quality processes."*** It was "the wild west;" you could roll code whenever you wanted there. He added that when he joined CrowdStrike, ***"there was no process in place anywhere"*** for quality assurance.

[69] At CrowdStrike, Mr. Gardner reported to Juliana de Freitas, head of user experience ("UX"). Mr. Gardner has over 15 years of experience as a UX designer and developer. Mr. Gardner has been the sole designer at multiple startups and has worked for enterprise software companies with 7,000+ employees where he has overhauled massive product suites. Mr. Gardner's previous positions include Senior User Experience Designer at One Identity and Lacework, as well as Senior Front End Developer at Ancestry.com. Jeff Gardner, LinkedIn, https://www.linkedin.com/in/jeffreywgardner/.

65. Mr. Gardner confirmed that it is industry standard for companies, such as CrowdStrike, to have a separate environment for development and staging to test software prior to deployment in the production environment. Mr. Gardner explained that the staging environment (which is also known as a pre-production environment) should mimic the production environment as closely as possible, and that updates being tested in such an environment should be as close to reality as possible. Mr. Gardner explained that, at CrowdStrike, there were no such checks to ensure the software his team worked with was tested in such an environment prior to deployment, and he saw no indication that a staging environment existed at CrowdStrike.

66. CrowdStrike itself has now admitted that it failed to test Rapid Response updates in a pre-production environment before rolling them out to customers, which ultimately caused the largest IT outage in history. Upon questioning by Congress after the Class Period, Adam Meyers (CrowdStrike's Senior Vice President of Counter Adversary Operations) admitted that CrowdStrike's updates were ***not "tested internally before [being] rolled out to customers."***[70] CrowdStrike further admitted that this failure was ***not*** the result of a rogue employee, but rather the product of CrowdStrike's intentional decision: the Company did not test Rapid Response updates in a pre-production environment, despite industry consensus that such testing is necessary.

67. Making matters worse, CrowdStrike not only failed to conduct tests of new software updates in a pre-production environment, the tests (if any) they performed outside of the pre-production environment were unreliable. FE 3 explained that CrowdStrike frequently encountered "flaky tests"—i.e., tests that result in a high number of false positives or negatives,

[70] Adam Meyers testimony at the Sept. 24, 2024 hearing before The House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection, https://www.youtube.com/watch?v=T-Ih1zu18XY.

and are thus indeterminate.[71] FE 3 explained that, as a result, CrowdStrike's engineers were never really sure if there were flaws in the software or if the test, itself, was flaky.[72] FE 3 added that the volume of flaky tests at CrowdStrike led to a breakdown of trust in the continuous integration pipeline because software engineers could never really identify the true issues. He noted that flaky tests were endemic to CrowdStrike while he was there. FE 3 communicated his personal concerns about these flaky tests to his manager, who told FE 3 that he had brought the issue up with his management as well, and that he was shocked that a company the size of CrowdStrike was dealing with these flaky tests. FE 3 explained that the sheer volume of flaky tests at CrowdStrike was the result of CrowdStrike pushing "speed over everything else."

68. **Second**, untold to investors during the Class Period, CrowdStrike failed to conduct phased rollouts (also known as "canary" rollouts) of its software updates—notwithstanding their public representations that they "always" conducted them. FE 1 reported that CrowdStrike did not conduct phased rollouts for its software updates, which he explained was a problem. FE 2 added that the standard practice in the industry is to employ a canary rollout, rolling out new updates first to either a small portion of customers or one specific region of customers and then monitoring the update's performance on customer systems for 24 to 48 hours. FE 3 similarly confirmed that it is not industry practice to roll out a content update to all customers simultaneously, because if there is something catastrophic, you would like to at least limit the number of people affected by it. Despite telling investors that it abided by this industry standard—with CrowdStrike stating that "we ***always*** do canary deployments of new services before rolling out changes to the entire fleet"—

[71] FE 3 was a Software Engineer at CrowdStrike from July 2022 to March 2023. FE 3 reported to Matthew Becker, a software development manager, who reported to Satyajit Nath.

[72] As FedRAMP explains, "[a] high density of [testing] false positives, indicates a potential problem with the analysis process or the analysis tool."

the Company did not do so.[73] Instead, it released its software updates to ***every*** customer simultaneously and ***without*** checking the impact. As Mr. Meyers (CrowdStrike's Senior Vice President) admitted to Congress, these software updates were ***"distributed to all customers in one session."***[74]

69. Even more, CrowdStrike's software updates were released to all CrowdStrike customers, ***regardless*** of whether they ***had opted out*** of receiving automatic updates. For example, Delta Air Lines "had not enabled its automatic update settings for CrowdStrike," but instead told CrowdStrike to allow Delta to "control installations and updates onto Delta's infrastructure."[75] Nevertheless, CrowdStrike's Rapid Response updates were pushed out to CrowdStrike customers who opted out of receiving automatic updates. As cybersecurity expert Alex Stamos explained, "I haven't seen anybody update the kernel in such a way [as CrowdStrike did]—and definitely not in a way that doesn't go through customer approval, as well. ... You're [supposed to be] giving customers the ability to control what's deployed, when it's deployed, what version is deployed, rollback capabilities, gradual rollout, phased deployments. All of those are kind of table stakes."[76] CrowdStrike, likewise, acknowledged after the Class Period that it should have given customers "control over the delivery of Rapid Response content updates," and vowed to do so going forward.[77]

---

[73] *Unexpected Adventures in JSON Marshaling*, CrowdStrike.com, https://www.crowdstrike.com/en-us/blog/unexpected-adventures-in-json-marshaling/.
[74] Adam Meyers testimony at the Sept. 24, 2024 hearing before The House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection, https://www.youtube.com/watch?v=T-Ih1zu18XY.
[75] Complaint at ¶ 43, *Delta Air Lines, Inc. v. CrowdStrike, Inc.*, No. 24-cv-013621 (Ga. Super. Ct. Oct. 25, 2024), ECF No. 1.
[76] Kyle Alspach, *SentinelOne CEO On CrowdStrike Outage: 'Not Just An Honest Mistake'*, CRN (July 30, 2024), https://www.crn.com/news/security/2024/sentinelone-ceo-on-crowdstrike-outage-not-just-an-honest-mistake.
[77] *Preliminary Post Incident Review (PIR)*, CrowdStrike (July 24, 2024).

70. **Third**, contrary to Defendants' representations to investors, CrowdStrike did ***not*** have a quality assurance team and did ***not*** have test plans for its software updates. FE 4 explained that CrowdStrike did not have a quality assurance team during his tenure at the Company.[78] FE 5, a former Onboarding Technical Account Manager and Provisioning Engineer at CrowdStrike, corroborated this account, explaining that CrowdStrike lacked a dedicated quality assurance team, and agreed that Defendants Kurtz and Sentonas would have known that fact.[79] FE 5 explained that it is strange to see a software company without a quality assurance team, especially with the number of releases CrowdStrike does. FE 1 also reported that CrowdStrike did not have a dedicated quality assurance team, adding that, with a kernel driver in cyber security, the risks are too high for there to be no dedicated quality assurance team. Mr. Gardner added that the industry standard is to have a code quality assurance person in between the developer and the production environment, but that there were no quality assurance engineers at CrowdStrike testing developers' code before the developers deployed such code to the production environment.

71. Likewise, FE 3 stated that, based on his experience, there was no dedicated quality assurance team at CrowdStrike. FE 3 reported that it was "baffling" that CrowdStrike did not have a dedicated quality assurance team. He added that Defendant Kurtz was driving a culture of fear, and that this culture of fear led to a desire to go to market as fast as possible, and that quality

[78] FE 4 was the Director of Engineering for infrastructure from April 2021 to September 2022. FE 4 reported to Alan Hannan and later Keith Culley, who reported directly to Chief Product Officer Amol Kulkarni. FE 4 was responsible for everything below the application software, including the building of the operating system, all the networks, everything from procurement and contracts to what the specs are of the servers they were going to buy, negotiating contracts for best price, developing storage architecture, and site selection for data centers.

[79] FE 5 was a Provisioning Engineer who worked at CrowdStrike from February 2021 to May 2024. As a Provisioning Engineer, FE 5 assisted with software development and assisted with patching faulty software updates.

assurance was in the way of that. FE 3 explained that the culture of speed over everything else that Defendant Kurtz created resulted in the lack of quality assurance at CrowdStrike.

72. CrowdStrike's former employees also described how the Company did not create "test plans" for software updates, even though industry standards required them. FE 6 was a Program Manager in the Engineering Department at CrowdStrike from August 2020 through May 2024.[80] FE 6 was responsible for running projects from start to finish. Based on his experience in the software industry, FE 6 would normally expect to see test plans before a software update was released, which would list and describe the tasks that must be completed before the update is pushed out to customers. However, as FE 6 explained, CrowdStrike's normal course of business was to proceed without a test plan for sensor releases.

73. CrowdStrike's failure to create test plans was consistent with its mission to maximize short-term profits by prioritizing speed over responsible testing. As FE 6 explained, the culture at CrowdStrike was "break fast, fix later," with a testing culture that was "very lax." The Company's aim, as FE 6 explained, was to "get it out the door as quickly as possible," at the expense of proper testing. FE 6 recounted that Defendant Sentonas would constantly tell CrowdStrike's engineering teams that they needed to move more quickly and would blame them for any issues the sales team had. According to FE 6, Defendant Sentonas would tell CrowdStrike's engineers that the sales team puts up half their salaries every month, and if they could not push products out fast enough, it would cost them their salaries.

74. Meanwhile, CrowdStrike's employees went out of their way to warn Defendants about the Company's failure to test software updates, failure to dedicate the necessary resources

[80] FE 6 was a Program Manager in the Engineering Department at CrowdStrike from August 2020 through May 2024. As a Program Manager, FE 6 was responsible for helping run projects from start to finish. FE 6 worked on projects related to sensor and cloud-based software updates.

to quality assurance, and failure to roll software updates out safely. Indeed, FE 5 sent an email around March 2024 with a video message to CEO George Kurtz, Mike Sentonas, and a few other members of upper management. FE 5's message to them explained that CrowdStrike employees would only be able to address critical issues if they were offered more support. FE 5 was told by the Vice President of Customer Success Paul McNulty that Defendants Kurtz and Sentonas saw his video message, but they did not act on it. When FE 5's concerns were ignored, he resigned from CrowdStrike.

75. These accounts are further corroborated by those contained in an exposé authored by investigative journalists at Semafor following the Class Period (the "Semafor Report").[81] The Semafor Report identified "[a]lmost ***two dozen*** former software engineers, managers and other staff [at CrowdStrike who] described a workplace where executives prioritized speed over quality, workers weren't always sufficiently trained, and mistakes around coding and other tasks were rising."[82] CrowdStrike's "former employees said quality checks on software were rushed at times to get products launched quickly."[83] CrowdStrike's software engineers detailed how they "complained about rushed deadlines, excessive workloads, and increasing technical problems to higher-ups ***for more than a year*** before [the] catastrophic failure of its software paralyzed airlines and knocked banking and other services offline for hours."[84] Among others, Preston Sego

[81] Lead Counsel spoke with the author of the Semafor Report, Rachyl Jones. Ms. Jones confirmed that she personally spoke to the people referenced in the Semafor Report, and the report reflected what they said. Ms. Jones further confirmed that none of the individuals referenced in the report with whom she spoke, who were critical of CrowdStrike, contacted her after the report's publication to say that they disagreed with the report or said that it twisted their words.
[82] Rachyl Jones, *CrowdStrike ex-employees: 'Quality control was not part of our process'*, Semafor (Sept. 12, 2024) at 3, https://www.semafor.com/article/09/12/2024/ex-crowdstrike-employees-detail-rising-technical-errors-before-july-outage.
[83] *Id.* at 5.
[84] *Id.* at 2.

recounted, based on his work at CrowdStrike from 2019 to 2023, that ***"[i]t was hard to get people to do sufficient testing sometimes."***[85] The Semafor Report, likewise, quoted Mr. Gardner, who confirmed that ***"[s]peed was the most important thing"*** at CrowdStrike and ***"[q]uality control was not really part of our process or our conversation."***[86] These "issues were raised during meetings, in emails, and in exit interviews."[87] Indeed, "[o]ne [CrowdStrike] former senior manager said they sat in multiple meetings where staff warned company leaders that ***CrowdStrike would 'fail' its customers by releasing products that couldn't be supported***."[88]

76. Defendants ignored their employees' concerns. They prioritized and emphasized "speed" to drive short-term profits at all costs, ignoring that they made representations to investors that they conducted pre-production testing and quality assurance procedures to ensure that Falcon "doesn't blue screen endpoints with failed updates."[89] Their choice to do so was severely reckless, at minimum, and—as discussed below—had devastating consequences on both CrowdStrike's customers and investors.

C. CrowdStrike Crashes Millions Of Systems Worldwide, And Customers And Investors Learn That CrowdStrike Failed To Sufficiently Test And Secure Its Falcon Updates

77. On Friday, July 19, 2024, a series of media reports revealed that CrowdStrike released a faulty Rapid Response update to the Falcon platform software that caused a worldwide IT outage, which crippled hospitals, schools, airlines, law enforcement agencies, Fortune 500

[85] Preston Sego worked at CrowdStrike from June 2019 to February 2023. At CrowdStrike, Mr. Sego's job was to review the tests completed by user experience developers that alerted engineers to bugs before proposed coding changes were released to customers. *Id.* at 5. Mr. Sego received a Bachelor of Science in Software Engineering from Rose-Hulman Institute of Technology in Terre Haute, Indiana. *See* Preston Sego, LinkedIn, https://www.linkedin.com/in/lprestonsegoiii.
[86] *Id.* at 2.
[87] *Id.* at 3.
[88] *Id.*
[89] Apr. 4, 2023 CrowdStrike Holdings, Inc. (CRWD) Investor Briefing transcript at 7.

companies, and more. That day, the *Wall Street Journal* reported that "[t]he outage touched almost every industry. Multiple financial institutions, government entities and corporations reported tech issues. Some hospitals and school districts said computers were down, and courthouses around the U.S. either closed or delayed trial proceedings."[90] *Bloomberg* added that behind the "massive IT failure that grounded flights, upended markets and disrupted corporations around the world is one cybersecurity company: CrowdStrike Holdings Inc."[91] Other experts and commentators agreed, dubbing it ***"the largest IT outage in history."***[92]

78. Defendant Kurtz publicly confirmed that CrowdStrike was, in fact, responsible for the global outage. He appeared on *NBC*'s Today Show on the day of the outage and stated that "[w]e're deeply sorry for the impact that we've caused to customers, to travelers to anyone affected by this, including our company." He added that "we know what the issue is," explaining that "the system was sent an update and that update had a software bug in it and caused an issue with the Microsoft operating system."[93] CrowdStrike then published a formal statement "sincerely apologiz[ing]" for the outage, admitting that "[t]he outage was caused by a defect found in a Falcon content update for Windows hosts."[94]

---

[90] Sam Schechner, Gareth Vipers, and Alyssa Lukpat, *Major Tech Outage Grounds Flights, Hits Banks and Businesses Worldwide*, The Wall Street Journal (July 19, 2024), https://www.wsj.com/tech/microsoft-reports-major-service-outage-affecting-users-worldwide-328a2f40.

[91] Jordan Robertson and Shona Ghosh, *Global IT Failure Puts Cyber Firm CrowdStrike in Spotlight*, Bloomberg (July 19, 2024), https://www.bloomberg.com/news/articles/2024-07-19/global-it-collapse-puts-cyber-firm-crowdstrike-in-spotlight.

[92] Rebecca Schneid, *CrowdStrike's Role In the Microsoft IT Outage, Explained*, https://time.com/7000476/microsoft-it-outage-crowdstrike-role-what-happened-explanation/.

[93] CrowdStrike CEO: 'We know what the issue is' and are resolving it, Today Show (July 19, 2024), https://www.today.com/video/crowdstrike-ceo-shares-what-spurred-global-outage-215232069726.

[94] *Our Statement on Today*, CrowdStrike (July 19, 2024).

79. Defendants Kurtz's and CrowdStrike's "apologies" and "explanations" were unsatisfactory to investors and the many customers impacted by the massive IT outage. As the host of *NBC*'s Today Show noted in disbelief during her interview of Defendant Kurtz, ***"How is it that one single software bug can have such a profound and immediate impact?"***[95]

80. Industry experts have described how Defendants failed to follow the basic, well-established procedures that they publicly represented CrowdStrike had in place during the Class Period. Indeed, as Professor Justin Cappos of New York University has explained, CrowdStrike's software updates were pushed out in ***"a very irresponsible way."***[96] Professor Cappos added that he was ***"astounded"*** by CrowdStrike's lack of appropriate testing of software updates "because there are lots and lots of other companies that are using industry standards and techniques in order to do this." Professor Cappos further explained, ***"This is not a hard problem…. It is unconscionable that they could still have these issues in 2024."***

81. Cybersecurity expert Alex Stamos, who was the former chief security officer at Facebook and is now the chief security officer of SentinelOne, explained that any "narrative" that this outage "could happen to anybody is false," as ***"CrowdStrike has made intentional architectural, engineering, and QA decisions that made this happen"*** and ***"they created this problem for themselves and the world."***[97] As to why CrowdStrike failed to adhere to basic

---

[95] Today Show (July 19, 2024), https://www.today.com/video/crowdstrike-ceo-shares-what-spurred-global-outage-215232069726.

[96] *See* Shannon Ferry, *NYU professor talks impact of global technology outage*, Spectrum News (July 19, 2024), https://ny1.com/nyc/all-boroughs/news-all-day/2024/07/19/nyu-professor-talks-impact-of-global-technology-outage. Professor Cappos is a professor in the Computer Science and Engineering department at New York University. Professor Cappos' research focuses on improving real world systems, often by addressing issues that arise in practical deployments. *See* https://engineering.nyu.edu/faculty/justin-cappos.

[97] *See* Risky Business Media, *Why CrowdStrike's Baffling BSOD Disaster Was Avoidable*, YouTube (July 29, 2024), https://www.youtube.com/watch?app=desktop&v=EGRqtscp4eE.

industry standards and conduct necessary tests, Professor Bruce Schneier of Harvard University explained that ***"it really is fundamentally economics. The business incentive is to grow and become critical, and then run as lean as absolutely possible."***[98]

82. CrowdStrike's failure to test its updates in a pre-production environment violated basic industry standards. As Mr. Stamos explained, it "is amazing" that the CrowdStrike update "never touched an actual running Windows machine" before it was released."[99] Mr. Stamos added that SentinelOne, which also sells cybersecurity software, conducts "thousands and thousands of tests" of content updates, using "real virtual machines and real hardware, then we roll it out to ourselves … before we roll it out to anyone else." Principal Product Manager at Microsoft, Bruno Borges, added, "I would have expected that CrowdStrike was dogfooding [i.e., testing in a pre-production environment] their own product in their employees' computers. ***That should've been the first pool of PCs in a canary deployment to test an update***."[100]

83. Mark Scheck, CEO and Chief Technology Officer of the cybersecurity company Amyrlin Technologies, likewise explained that "CrowdStrike didn't seem to test this update thoroughly or at all. It affected their entire Windows customer base. ***If they had tested it, they***

[98] *See How a software update sparked tech disruptions worldwide*, PBS News Hour (July 19, 2024), https://www.pbs.org/video/global-outage-1721424405/. Professor Schneier is an Adjunct Lecturer in Public Policy at the Harvard Kennedy School and a Fellow at the Berkman Klein Center for Internet & Society. He is a board member of the Electronic Frontier Foundation, Access Now, and The Tor Project; and an advisory board member of Electronic Privacy Information Center. He is the author of several books on computer security. *See* https://www.hks.harvard.edu/faculty/bruce-schneier.

[99] Risky Business Media, *Why CrowdStrike's Baffling BSOD Disaster Was Avoidable*, YouTube (July 29, 2024), https://www.youtube.com/watch?app=desktop&v=EGRqtscp4eE.

[100] @brunoborges, X.com. Bruno Borges is a Principal Product Manager at Microsoft. Mr. Borges's prior positions include Principal Cloud Advocacy Manager at Microsoft, Principal Product Manager at Oracle, and Chief Technology Officer and Co-founder at Comprei e Não Vou. *See* Bruno Borges, LinkedIn, https://www.linkedin.com/in/brunocborges/?originalSubdomain=ca/.

would have found that this update bricks Windows 10 machines and causes the [blue screen]."[101] He added that the failure to test in a production environment ***"likely related to [CrowdStrike's] corporate culture."*** Matthew Rosenquist, Chief Information Security Officer at Mercury Risk (formerly Intel Corporation), agreed that the revelations made clear that CrowdStrike's Rapid Response updates "are ***not*** thoroughly tested before landing on systems and they instead rely on endpoint [i.e., customer] functions to handle any residual problems."[102] Mr. Rosenquist noted that this "is a ***serious process design failure*** for their product Quality Assurance," adding that "CrowdStrike should be properly testing every piece of code that is sent to client machines" and its failure to do so was ***"egregious."*** Theo Browne, a software engineer and cybersecurity expert, similarly explained that ***"if CrowdStrike had just checked that this update had run on <u>one</u> machine successfully <u>one</u> time before sending it out, this would not have happened."***[103]

[101] Mr. Scheck is the founder of Amyrlin Technologies, a cybersecurity company. He was previously the director of DevOps at multiple companies, including WWE and Shapeways. He is an AWS Certified Cloud Practitioner. *See* Mark Scheck, *Why Did The CrowdStrike Incident Happen and Where Do We Go From Here*, LinkedIn (July 24, 2024), https://www.linkedin.com/pulse/why-did-crowdstrike-incident-happen-where-do-we-go-from-mark-scheck-rcine/.

[102] *See* Matthew Rosenquist, *Learning from CrowdStrike's quality assurance failures*, Help Net Security (July 25, 2024), https://www.helpnetsecurity.com/2024/07/25/crowdstrike-quality-assurance-failures/. Mr. Rosenquist is the Chief Information Security Officer at Mercury Risk. Mr Rosenquist has held numerous other positions in the cybersecurity field, including Cybersecurity Strategist – Artificial Intelligence Group and Security Strategic Planner at Intel Corporation, as well as Chief Information Security Officer at Eclipz.io, Inc. Mr. Rosenquist serves as an Advisory Board Member – Committee for the Master of Science in Information Security at Brandeis University. *See* Matthew Rosenquist, LinkedIn, https://www.linkedin.com/in/matthewrosenquist/details/experience/.

[103] *See* Diving into the embarrassing engineering behind CrowdStrike, YouTube (July 25, 2024), https://www.youtube.com/watch?v=7rx4U5TlaqE. Theo Browne host a YouTube show on cybersecurity development. Mr. Browne has held the positions of Founder & CEO at Ping Labs, Lead Developer and Founding Member at Turntable Labs, and Software Engineer at Twitch. Mr. Browne holds a degree in Computer Science from Rensselaer Polytechnic Institute. *See* Theo Browne, LinkedIn, https://www.linkedin.com/in/t3gg/.

84. Industry experts also identified CrowdStrike's abject failure to properly test its updates as a violation of the very NIST industry standards that underlie the FedRAMP and DoD requirements that Defendants repeatedly assured investors that CrowdStrike adhered to. As stated above, the NIST requires that when testing new software updates, "[c]onfigurations in the test environment mirror the configurations in the operational environment to the extent practicable so that the results of the testing are representative of the proposed changes to the operational systems."[104] As Robert Thomas, cybersecurity expert and former DoD staffer, explained, had CrowdStrike followed the NIST's testing requirements, "the flaws in the update should have become apparent before it was circulated to users."[105] Mr. Thomas added that CrowdStrike violated "the basics" for "patches, updates, and on critical business systems."[106]

85. As industry experts have further explained, CrowdStrike's failure to conduct phased rollouts of its software updates also violated basic industry standards, as well as CrowdStrike's public assurances that they "always" conducted such phased rollouts before releasing the update "to the entire fleet."[107] Professor Bruce Schneier of Harvard University specifically chastised CrowdStrike for its failure to conduct the phased rollouts Defendants assured investors the Company performed, explaining that ***"CrowdStrike could have rolled out this***

---

[104] U.S. Dept. of Defense (Apr. 11, 2016), https://www.dcsa.mil/Portals/91/Documents/CTP/NAO/JSIG_2016April11_Final_(53Rev4).pdf.

[105] Kevin Stocklin, *After CrowdStrike Outage, Companies and Governments Reassess Risks of Using Cloud*, Tech Talk Summits, https://techtalksummits.com/news/cybersecurity/after-crowdstrike-outage-companies-and-governments-reassess-risks-of-using-cloud. Robert Thomas is a Principal at 180AConsulting, a cybersecurity and IT program management consulting firm. Mr. Thomas's past positions include Chief Information Security Officer at Pacific Star Communications, Inc., Director of Cybersecurity at Radisys Corporation, Security and Compliance Architect for a contractor of the U.S. Department of Energy, and Military Intelligence Warrant Officer. *See* Robert Thomas, LinkedIn https://www.linkedin.com/in/leaderwithvision/.

[106] *Id.*

[107] *Unexpected Adventures in JSON Marshaling*, CrowdStrike.com, https://www.crowdstrike.com/en-us/blog/unexpected-adventures-in-json-marshaling/.

change incrementally and caught this before it became a disaster."[108] Professor Feng Li, Associate Dean for Research and Innovation and Chair of Information Management at Bayes Business School in London, agreed, explaining, "What's especially surprising is that CrowdStrike didn't carry out staged rollouts of this update—usually, you'd roll out to a small percent first…. That way, any problems can be spotted, and things can be paused or rolled back before it causes massive damages."[109]

86. Following the CrowdStrike outage, industry experts also noted the "uncanny" similarities between the outage caused by CrowdStrike's faulty update and the outage caused by McAfee's faulty update years earlier—both of which occurred on Defendants Kurtz's and Sentonas's watch. As discussed above, Defendants Kurtz and Sentonas were both the Chief Technology Officers of McAfee, with Kurtz claiming he had "learned this lesson at ... McAfee."[110] While they were key leaders at McAfee, that company similarly failed to test a software update in a pre-production environment prior to its release and failed to conduct a phased rollout of its software update, causing hundreds of thousands of blue screens on customer computers. As industry experts explained following the CrowdStrike outage, Defendant Kurtz's and Sentonas's

[108] William Brangham and Nana Adwoa Antwi-Boasiako, *How a faulty software update sparked tech disruptions worldwide*, PBS (July 19, 2024), https://www.pbs.org/newshour/show/how-a-faulty-software-update-sparked-tech-disruptions-worldwide.

[109] *Expert Reaction to CrowdStrike IT Disaster*, City University of London (July 19, 2024), https://www.city.ac.uk/news-and-events/news/2024/july/expert-reaction-to-crowdstrike-it-disaster#:~:text=Robust%20operating%20systems%20needed,for%20companies%20that%20use%20CrowdStrike. Professor Feng Li, PhD, is the Associate Dean, Research and Innovation and Chair of Information Management at Bayes Business School. Professor Li's research focuses on how digital technologies can be used to facilitate strategic innovation. Professor Li also advises senior business leaders and policy makers on how to manage the transition to new technologies. *See* https://www.bayes.city.ac.uk/faculties-and-research/experts/feng-li.

[110] Mar. 7, 2024 Morgan Stanley Technology, Media & Telecom Conference transcript at 4.

failures at CrowdStrike and McAfee were ***"eerily similar,"***[111] referring to the CrowdStrike outage as ***"the 2024 sequel."***[112] These industry experts openly asked, ***"how Kurtz, with all his experience, let something like this happen again at CrowdStrike."***[113]

D. Investors Suffer Losses When They Learn That CrowdStrike Failed To Sufficiently Test And Secure Its Falcon Updates

87. Defendants' misstatements and omissions concerning CrowdStrike's practices for software updates have caused immense harm to investors. As the financial press has explained, "[s]hares of CrowdStrike went over a cliff after it became clear that the company was to blame" for the historic outage.[114] Indeed, on Friday, July 19, 2024, following the news reports and admissions by Defendant Kurtz revealing that CrowdStrike released a faulty update to its Falcon Platform software that day causing customer computers to blue screen, the Company's share price fell $38.09, wiping out billions of dollars in shareholder value. As analysts at J.P. Morgan wrote that evening, "[o]vernight, we learned that CRWD users have been experiencing global Microsoft outage issues related to a software update that seems to be connected to CrowdStrike's Falcon platform for Windows."[115] Analysts at Wells Fargo agreed, concluding that the outage was ***"self-***

---

[111] Adrian Volenik, *CrowdStrike CEO Was Working For McAfee In 2010 When There Was A Global Tech Outage Too*, Benzinga (July 25, 2024), https://finance.yahoo.com/news/crowdstrike-ceo-involved-another-global-200015346.html.

[112] Ed Bott, *What caused the great CrowdStrike-Windows meltdown of 2024? History has the answer*, ZDNet (July 24, 2024), https://www.zdnet.com/article/what-caused-the-great-crowdstrike-windows-meltdown-of-2024-history-has-the-answer/.

[113] Adrian Volenik, *CrowdStrike CEO Was Working For McAfee In 2010 When There Was A Global Tech Outage Too*, AOL (July 25, 2024), https://www.aol.com/crowdstrike-ceo-involved-another-global-220015512.html.

[114] David Jagielski, *Is CrowdStrike a Bad-News Buy?*, The Motley Fool (Sept. 5, 2024), https://www.fool.com/investing/2024/09/05/is-crowdstrike-a-bad-news-buy/.

[115] July 19, 2024 J.P. Morgan analyst report, *Outage Disruptive But A Long-Term Buying Opportunity*.

inflicted" and expressing concern "with the impact it will have on future demand trends, as it will not likely be easy to recover quickly from this."[116]

88. Over that weekend, investors learned more about the reasons for the CrowdStrike outage, and what the causes revealed about CrowdStrike's failures to comply with the very standards to which Defendants represented that the Company adhered. On Saturday, July 20, 2024, Jen Easterly, director of the United States Cybersecurity and Infrastructure Security Agency, said the outage "was a huge deal with serious impacts on critical infrastructure operations across the world," adding that "[a]ny company that builds any kind of software should design, test and deliver it with a priority on dramatically driving down the number of flaws."[117] *Bloomberg* further noted that the outage was ***"the most catastrophic IT failure the world has ever seen."***[118] That same day, Microsoft disclosed that an estimated ***8.5 million*** computers running Windows were affected by CrowdStrike's failure to adhere to their represented safeguards for software updates. Then, on Monday, July 22, 2024, members of the Congressional Committee on Homeland Security called Defendant Kurtz to testify, with Congress explaining that ***"Americans will undoubtedly feel the lasting, real-world consequences of this incident"*** and ***"deserve to know in detail how this incident happened and the mitigation steps CrowdStrike is taking."***[119]

---

[116] July 19, 2024 Wells Fargo analyst report, *CrowdStrike Creates Global Outage, Likely to Create Liabilities and Demand Issues*.

[117] Katrina Mason, *CrowdStrike's Mistake Was a 'Huge Deal,' US Cyber Official Says*, Bloomberg https://www.bnnbloomberg.ca/business/company-news/2024/07/20/crowdstrikes-mistake-was-a-huge-deal-us-cyber-official-says/.

[118] Lynn Doan & Matt Day, *CrowdStrike Crash Affected 8.5 Million Microsoft Windows Devices*, Bloomberg (July 21, 2024), https://www.ndtvprofit.com/business/crowdstrike-crash-affected-8-5-million-microsoft-windows-devices.

[119] Letter from Committee on Homeland Security to George Kurtz (July 22, 2024), https://homeland.house.gov/wp-content/uploads/2024/07/CrowdStrike-Software-Update-Letter_FINAL.pdf.

89. CrowdStrike's stock price fell further following these additional revelations, as investors learned more about the Company's failure to adhere to basic industry standards for testing and quality assurance, as well as the natural consequence of those failures. On Monday, July 22, 2024, the first full trading day after the IT outage, the Company's stock dropped again, this time by nearly 13.5%, from $304.96 to $263.91. The stock continued to fall over the coming days. All told, in response to the revelations about the outage and its implications, CrowdStrike's stock plummeted ***$109 per share***, nearly ***32%***, by July 30, 2024.

E. CrowdStrike Admits That It Failed To Conduct Necessary Tests And Secure Its Falcon Updates, Leading To Even More Investor Losses

90. Defendants had no choice but to accept responsibility for the global outage and admit that they failed to adhere to the practices they represented that they followed during the Class Period. Pressed by Congress and other stakeholders, CrowdStrike admitted that the outage was caused by its failure to conduct necessary tests in a pre-production environment of its software updates and its choice to simultaneously push its software update out to all customers in violation of industry-standard practices. CrowdStrike has now re-committed to following the basic standards for software updates that it previously assured customers and investors that it "always" followed.

91. Specifically, on July 24, 2024, CrowdStrike released a Preliminary Post Incident Review ("PIR") that purported to describe the underlying causes of the outage.[120] The PIR confirmed that CrowdStrike was ***not*** conducting necessary testing despite years of representations to the contrary. It further acknowledged that, had CrowdStrike conducted the tests it had for years represented were part of its routine process, the faulty update would have been caught prior to release. In addition, CrowdStrike committed to adopting pre-production environment testing and

[120] *Preliminary Post Incident Review (PIR)*, CrowdStrike (July 24, 2024).

phased rollouts for all future updates, thus re-committing to the very safety requirements Defendants had for years represented they complied with (but secretly shirked). Indeed, in a section of its PIR report titled "How Do We Prevent This From Happening Again?," CrowdStrike stated that it would begin conducting pre-production testing. Specifically, they stated that they would begin to conduct "[l]ocal developer testing"—i.e., testing in "a self-contained and isolated [environment] that allows software developers to … debug their applications on their own machines before deploying them to a production environment."[121] CrowdStrike added that it would also begin to "[i]mplement a staggered deployment strategy for Rapid Response Content in which updates are gradually deployed to larger portions of the sensor base, starting with a canary deployment."[122]

92. Notably, Defendants tried to sugarcoat and downplay CrowdStrike's deficiencies in their PIR and in the slightly more detailed External Technical Root Cause Analysis published on August 6, 2024.[123] Industry experts saw through the sugar-coating and rightfully understood CrowdStrike's post-mortem report as admissions that the Company's testing and quality assurance practices were deficient and ***not*** as previously represented. For example, Professor Toby Murray of the University of Melbourne's School of Computing and Information Systems, explained that "[t]he fact that the CrowdStrike developers were able to have this obvious inconsistency between the data file format and the software code ***means that the most basic forms of quality review and***

[121] *Id.*
[122] *Id.*
[123] *External Technical Root Cause Analysis — Channel File 291*, CrowdStrike (Aug. 6, 2024), https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf.

assurance were not being correctly carried out."[124] Professor Sigi Goode of the Australian National University similarly noted that, ***"when they wrote this [root cause analysis] report, they must have been feeling very embarrassed,"*** as "[f]irst-year programming students are taught" about the need to conduct phased deployment of software updates.[125] Industry commentators further concluded following CrowdStrike's PIR that ***"[t]oday, we learned two incredible things"*** that left them ***"slack jawed in horror"***—specifically, "CrowdStrike doesn't dogfood [i.e., test in a pre-production environment], nor do staged, 'canary' deployment."[126] As to CrowdStrike's commitment to conduct the necessary testing going forward, cybersecurity consultant Daniel Card poignantly noted in an article published by *Forbes*, ***"I'm happy to see they are going to change the design to be what it should have had in the first place."***[127]

---

[124] Annika Berges, *CrowdStrike releases root cause analysis of the global Microsoft breakdown*, ABC (Aug. 6, 2024), https://www.abc.net.au/news/2024-08-07/drt-crowdstrike-root-cause-analysis/104193866. Professor Toby Murray is a faculty member of the School of Computing and Information Systems at the University of Melbourne. Professor Murray's research "focuses on how to build highly secure computer systems using rigorous techniques, such as formal software verification and novel programming languages; and how to discover vulnerabilities in software and systems." Professor Murray holds a D.Phil. in Computer Science from the University of Oxford and a Bachelor of Computer Science from the University of Adelaide. *See* https://findanexpert.unimelb.edu.au/profile/780796-toby-murray.

[125] *Id.* Professor Sigi Goode is a Professor of Information Systems at the Australian National University. Professor Goode's research focuses on "information security behavior, services and technology adoption, policy and use." Professor Goode has more than fifteen years of experience designing and managing online information platforms. *See* Sigi Goode expert profile, https://researchportalplus.anu.edu.au/en/persons/sigi-goode.

[126] Richi Jennings, *CrowdStrike Admits it Doesn't 'Canary' Test all Updates*, Security Boulevard (July 24, 2024), https://securityboulevard.com/2024/07/crowdstrike-pir-canary-bsod-richixbw/#:~:text=The%20cause%20was%20a%20corrupt,staged%2C%20%E2%80%9Ccanary%E2%80%9D%20deployment.

[127] Mr. Card is a technology and cybersecurity expert "who has worked with organizations globally to help protect, detect, and respond to cyber threats. He is active in the UK cyber community, serving on the UK Government Cyber Security Advisory Board." *See The Pivot Podcast: A Real Deep Dive into the World of Cybersecurity with Daniel Card*, Pivot Podcast (Sept. 15, 2023), https://www.maltego.com/blog/the-pivot-podcast-a-real-deep-dive-into-the-world-of-cybersecurity-with-daniel-card/.

93. On August 10, 2024, Defendant Sentonas attended the Def Con hacking conference in Las Vegas, where he accepted the ***"Most Epic Fail"*** award on behalf of CrowdStrike for causing the global IT outage. According to the Def Con awards committee, the "Most Epic Fail" award is meant to "honor a person or corporate entity's spectacularly epic fail – the kind of fail that lets the entire infosec industry down in its wake."[128] The award is aimed at providing some solace to "the investors who … departed with eight-figure checks for a pitch presenting snake oil served over word salads on a fool's gold platter."[129] In accepting the award on behalf of CrowdStrike, Defendant Sentonas admitted it was ***"super important to own it when you do things horribly wrong, which we did in this case."*** He reiterated that ***"we got this wrong."***[130]

94. On September 24, 2024, CrowdStrike executive Adam Meyers testified on behalf of CrowdStrike before the House Subcommittee about the outage. CrowdStrike again attempted to downplay the seriousness of its testing, quality assurance, and software release deficiencies. Nevertheless, Mr. Meyers was forced to admit to certain of CrowdStrike's failings. During his testimony, Mr. Meyers confirmed that CrowdStrike did ***not*** test software updates in a pre-production environment prior to release to the public and did ***not*** conduct phased rollouts of its software updates. During the House Subcommittee hearing, Mr. Meyers stated CrowdStrike would ***now*** begin to conduct the required tests and follow the industry standard practices that CrowdStrike assured investors during the Class Period that it already did. Indeed, Mr. Meyers

[128] Pwnie Award Winners 2023, https://pwnies.com/winners/.
[129] *Id*.
[130] Amanda Yeo, *CrowdStrike accepts Pwnie Award for Most Epic Fail in person*, Mashable (Aug. 12, 2024), https://mashable.com/article/crowdstrike-outage-pwnie-award-epic-fail-acceptance-speech.

identified CrowdStrike's ***new*** "phased rollout approach and also the pre-deployment testing" as the primary "changes to [CrowdStrike's] internal practices to avert future, similar incidents."[131]

95. The fallout of the outage has continued to this day. On October 25, 2024, Delta Air Lines—one of CrowdStrike's largest and most sophisticated customers—filed a $500 million lawsuit against the Company, documenting how CrowdStrike lied to Delta and the public. In its complaint, which asserts claims for "deceptive and unfair business practices," Delta corroborated that CrowdStrike's software updates were not tested before being automatically rolled out to Delta's systems. As Delta explained, ***"CrowdStrike caused a global catastrophe because it cut corners, took shortcuts, and circumvented the very testing and certification processes it advertised, for its own benefit and profit."***[132] Delta further detailed how, "[t]o maintain the facade that it could safely deploy its solutions more rapidly than competitors, ***CrowdStrike touted compliance with operating system requirements, while altering previously certified computer programming with uncertified and untested shortcuts that damaged and impaired its clients' systems and businesses***." Delta stressed that "CrowdStrike ***never*** disclosed that it deployed computer programming and data that circumvented certifications, verifications, and testing, and Delta ***never*** gave CrowdStrike such permission."

96. In sum, while prioritizing speed over safety to drive short-term financial gains, Defendants misled investors and customers about their mission critical testing and quality assurance practices. Defendants' conduct has caused enormous losses to investors, including Lead Plaintiff.

---

[131] Adam Meyers testimony at the Sept. 24, 2024 hearing before The House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection, https://www.youtube.com/watch?v=T-Ih1zu18XY.

[132] Complaint at ¶ 3, *Delta Air Lines, Inc. v. CrowdStrike, Inc.*, No. 24-cv-013621 (Ga. Super. Ct. Oct. 25, 2024), ECF No. 1.

V. ADDITIONAL ALLEGATIONS OF SCIENTER

97. A host of additional facts support a strong inference that Defendants knew, or at minimum were severely reckless in not knowing, that their statements to investors were false or misleading by omission. These include the following:

98. ***The Falcon platform was CrowdStrike's only product.*** During the Class Period, CrowdStrike offered one product—its Falcon cybersecurity platform. All of its revenues were derived from its Falcon platform, and the Company's success (or failure) hinged entirely on its one platform. CrowdStrike has repeatedly acknowledged that its entire financial wellbeing depended on its ability to "convince potential customers to allocate a portion of their discretionary budgets to purchase our Falcon platform" and to convince existing customers to "renew their subscriptions for our Falcon platform."[133] As Defendant Sentonas has publicly acknowledged, "The Falcon platform is at the core of everything we do."[134] The significance of Falcon to CrowdStrike's bottom-line supports the scienter inference: Defendants knew or were, at minimum, severely reckless in not knowing about the Company's failure to properly test and roll out updates for its lone product that Defendants spoke to investors so extensively about.

99. ***Defendants repeatedly touted CrowdStrike's software testing.*** Defendants Kurtz and Sentonas took every opportunity to tell CrowdStrike customers and the investing public that their Company took the necessary steps to ensure that its software updates were safe, including that the Company conducted proper testing prior to releasing updates. For example, at the beginning of the Class Period, Defendant Kurtz assured investors that ***"[t]esting and validation is really important"*** at CrowdStrike and ***"[w]e test more than anyone else, more than all of our***

[133] *See, e.g.*, CrowdStrike 10-K for the fiscal year ended January 31, 2023 (Mar. 9, 2023).
[134] CTO Mike Sentonas: CrowdStrike Falcon Platform Tour (Nov. 30, 2020), https://www.youtube.com/watch?v=WmLU29pFdxw.

next-gen competitors, more than other players that are out there."[135] Defendant Kurtz further stressed to investors that CrowdStrike tested its updates in a pre-production environment prior to their release, stating that CrowdStrike made ***"sure that code is secure, that it's deployed and that it's run in a secure environment."***[136] During a later earnings call, Defendant Kurtz told investors that CrowdStrike's testing processes ensured CrowdStrike identified faulty coding in advance of deployment of updates, which further enabled CrowdStrike to prevent ***"insecure code [from] being put into the CICD pipeline."***[137] The fact that Defendants specifically and repeatedly held themselves out as knowledgeable authorities regarding CrowdStrike's software testing demonstrates that Defendants either knew these statements were false or misleading or were, at minimum, severely reckless in not investigating and knowing the truth about CrowdStrike's failure to conduct necessary and basic testing before making these statements.

100. ***Defendants repeatedly assured investors that CrowdStrike's software updates do not result in "blue screens."*** Defendants specifically positioned Falcon as unique because its updates did ***not*** cause "blue screens." For example, Defendant Sentonas told investors that Falcon software ***"doesn't blue screen endpoints with failed updates,"*** which was one ***"one of the most important things" to customers.***[138] Defendant Kurtz likewise told investors that CrowdStrike was able to sell its software to "many, many airlines" because its updates will ***not*** require its customer "to send out an IT person to go fix a kiosk that has a Microsoft blue screen."[139] Having specifically and repeatedly held themselves out as knowledgeable authorities regarding Falcon's "secure"

[135] Sept. 20, 2022 CrowdStrike Holdings, Inc. Presents at Fal.con 2022 transcript at 4.
[136] Sept. 5, 2023 CrowdStrike Holdings, Inc. Presents at Goldman Sachs Communacopia & Technology Conference transcript at 10.
[137] Aug. 30, 2023 CrowdStrike Holdings, Inc., Q2 2024 Earnings Call transcript at 15.
[138] Apr. 4, 2023 CrowdStrike Holdings, Inc. (CRWD) Investor Briefing transcript at 7.
[139] Nov. 28, 2023 Q3 2024 Earnings Call transcript at 16.

update process that "doesn't blue screen" customers' computers, Defendants either knew or were, at minimum, severely reckless in not knowing the true, undisclosed facts.

101. ***Defendants Kurtz and Sentonas claimed to have "learned their lesson" after failing to test and identify a faulty software update before releasing it to customers while at McAfee, crashing hundreds of thousands of customer computers.*** Prior to joining CrowdStrike, Defendants Kurtz and Sentonas were Chief Technology Officers at McAfee, another company that makes cybersecurity software. Under their leadership, McAfee distributed to its customers a software update that contained a coding error that caused tens of thousands of PCs across the world to crash and enter a reboot loop.[140] In response to the crash, McAfee admitted that the release of the faulty update was a failure of McAfee's quality assurance process leading to a "blue screen."[141] At the time, industry experts publicly observed that McAfee could have prevented the crash if it had tested the update in a pre-production environment before pushing it out to customers, describing such a process as ***"very basic testing, not something weird or intricate"*** and noting that ***"[t]he fact that McAfee didn't see this as part of normal testing is really shocking."***[142] Other industry experts also noted that McAfee's failure to conduct phased rollouts contributed to the

[140] Lance Whitney, *McAfee Apologizes for Antivirus Disaster*, CNet (Apr. 23, 2010), https://www.cnet.com/news/privacy/mcafee-apologizes-for-antivirus-update-disaster/.
[141] Barry McPherson, *An Update on False Positive Remediation*, McAfee Security Insights Blog (Apr. 22, 2010), http://web.archive.org/web/20100429010738/http://siblog.mcafee.com/support/an-update-on-false-positive-remediation; Ed Bott, *Defective McAfee Update Causes Worldwide Meltdown of XP PCs*, ZDNet (Apr. 21, 2010), https://www.zdnet.com/article/defective-mcafee-update-causes-worldwide-meltdown-of-xp-pcs/.
[142] Bryan Acohido, *Massive manual PC cleanup expected after McAfee error*, USA Today (Apr. 22, 2010), http://content.usatoday.com/communities/technologylive/post/2010/04/massive-manual-pc-cleanup-triggered-by-mcafee-error/1.

crash, explaining that "this just goes to show how important it is to download new updates to one machine to test it first before rolling out to the whole fleet."[143]

102. During the Class Period, Defendant Kurtz made clear that such an outage would not occur at CrowdStrike, telling investors that he had ***"learned this lesson … at McAfee."***[144] As industry experts noted after the CrowdStrike outage and once they learned of CrowdStrike's woefully deficient testing of its software updates, "[t]he parallels between that [McAfee] incident and this year's CrowdStrike outage are uncanny."[145] The two outages were "eerily similar,"[146] with industry experts referring to the CrowdStrike outage as "the 2024 sequel."[147] These experts justifiably questioned with incredulity ***"how Kurtz, with all his experience, let something like this happen again at CrowdStrike."***[148] Defendants' prior experience releasing an untested and faulty update at McAfee, which caused a similarly severe mass outage, further strengthens the scienter inference. Defendants either knew or were, at minimum, severely reckless in not knowing that CrowdStrike also did not test its software updates in a production environment before releasing them simultaneously to all of their customers.

---

[143] Ed Bott, *What caused the great CrowdStrike-Windows meltdown of 2024? History has the answer*, ZDNet (July 24, 2024), https://www.zdnet.com/article/what-caused-the-great-crowdstrike-windows-meltdown-of-2024-history-has-the-answer/.
[144] Mar. 7, 2024 Morgan Stanley Technology, Media & Telecom Conference transcript at 4.
[145] Ed Bott, *What caused the great CrowdStrike-Windows meltdown of 2024? History has the answer*, ZDNet (July 24, 2024), https://www.zdnet.com/article/what-caused-the-great-crowdstrike-windows-meltdown-of-2024-history-has-the-answer/.
[146] Adrian Volenik, *CrowdStrike CEO Was Working For McAfee In 2010 When There Was A Global Tech Outage Too*, Benzinga (July 25, 2024), https://finance.yahoo.com/news/crowdstrike-ceo-involved-another-global-200015346.html.
[147] Ed Bott, *What caused the great CrowdStrike-Windows meltdown of 2024? History has the answer*, ZDNet (July 24, 2024), https://www.zdnet.com/article/what-caused-the-great-crowdstrike-windows-meltdown-of-2024-history-has-the-answer/.
[148] Adrian Volenik, *CrowdStrike CEO Was Working For McAfee In 2010 When There Was A Global Tech Outage Too*, AOL (July 25, 2024), https://www.aol.com/crowdstrike-ceo-involved-another-global-220015512.html.

103. ***CrowdStrike violated basic industry standards governing the software development process that any industry participant would recognize as fundamental.*** The software development testing, quality assurance, and rollout processes that CrowdStrike failed to conduct are not complex, intricate, or debatable. Industry experts resoundingly agree that testing software changes in pre-production environments, maintaining dedicated quality assurance staff to administer reliable and consistent test plans, and rolling updates out in phases are basic, universal, and well-established industry requirements. As Professor Toby Murray explained CrowdStrike was not conducting ***"the most basic forms of quality review and assurance."***[149] Professor Sigi Goode similarly noted these basic industry standards are well-understood by ***"[f]irst-year programming students."***[150]

104. Indeed, Defendants themselves acknowledged the importance of adhering to these well-recognized and basic standards for software development and release. Both before and during the Class Period, CrowdStrike stressed that software updates should only be released after they were tested in "a staging environment that closely resembles the production environment."[151] Defendant Kurtz confirmed that such testing is essential because you have to "make sure that you're not putting tainted containers and vulnerabilities into your pipeline."[152] Similarly, CrowdStrike assured the public that "for system stability, we ***always*** do canary deployments of

[149] Annika Berges, *CrowdStrike releases root cause analysis of the global Microsoft breakdown*, ABC (Aug. 6, 2024), https://www.abc.net.au/news/2024-08-07/drt-crowdstrike-root-cause-analysis/104193866.
[150] *Id.*
[151] *What is CI/CD?: Pipeline Benefits and Tools*, CrowdStrike.com (July 4, 2024), https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/continuous-integration-continuous-delivery-ci-cd/.
[152] Dec. 8, 2022 CrowdStrike Holdings, Inc. Presents at Barclays 2022 Global Technology, Media and Telecommunications Conference transcript at 11.

new services before rolling out changes to the entire fleet."[153] That Defendants held themselves out as knowledgeable of these basic tenets of safe software update development and release—yet blatantly violated them—further strengthens the inference of, at minimum, severe recklessness.

105. ***The absence of any quality assurance team at CrowdStrike was obvious and known.*** As discussed above, Defendants represented that they had a "quality assurance team," which was supposedly "trained and equipped to assist with testing."[154] But numerous former employees recounted how CrowdStrike did ***not*** have a quality assurance team, which was particularly "strange" with the "risks too high." The absence of a quality assurance team was obvious to anyone at the Company—particularly those responsible for decision-making and corporate strategy. Defendants either knew or were, at minimum, severely reckless in not knowing the true, undisclosed fact that CrowdStrike lacked the quality assurance team that they repeatedly told investors they had.

106. ***CrowdStrike executives, including Defendants Kurtz and Sentonas, certified to FedRAMP in sworn declarations that the Company met FedRAMP requirements to test in a pre-production environment and maintain a dedicated quality assurance.*** FedRAMP specifically requires software companies doing business with the government, such as CrowdStrike, to test updates in a pre-production environment before releasing them. Specifically, FedRAMP requires testing "in a separate test environment before implementation in an operational environment" and that such environment should consist of "operational systems" or a close "replication" of such systems. Likewise, the DoD specifically required CrowdStrike to "verify

---

[153] *Unexpected Adventures in JSON Marshaling*, CrowdStrike.com, https://www.crowdstrike.com/en-us/blog/unexpected-adventures-in-json-marshaling/.

[154] CrowdStrike Environmental, Social and Governance Initiatives, https://www.crowdstrike.com/wp-content/uploads/2024/01/crowdstrike-esg-initiatives.pdf.

proposed configuration changes prior to implementation in the operational environment." Additionally, FedRAMP and DoD both required CrowdStrike to comply with the NIST's requirement to test software updates in a "test environment" that "mirror[s] the configurations in the operational environment to the extent practicable so that the results of the testing are representative of the proposed changes to the operational systems."[155] FedRAMP and DoD also required CrowdStrike to comply with the NIST's requirement to maintain a dedicated quality assurance team to exclusively conduct "quality assurance and testing."[156] Defendants represented to investors that CrowdStrike was "[m]eeting [these] stringent requirements," and repeatedly touted their compliance with these requirements as a reason to buy the Company's stock.

107. In fact, Defendants were specifically obligated to sign sworn verifications that they were complying with these requirements. As explained above (¶ 55), FE 8 confirmed that Defendant Kurtz, or someone else in CrowdStrike's C-Suite, including Defendant Sentonas had to sign certifications attesting to CrowdStrike's compliance with these requirements. That Defendants were obligated to, represented publicly (falsely) that they did, and personally certified (falsely) to the government that they did, comply with the government's requirements for software development further strengthens the scienter inference.

108. ***CrowdStrike's employees warned Defendants that the Company did not conduct adequate testing and lacked sufficient quality assurance.*** Employees sounded the alarm within CrowdStrike about the deficient testing and quality control in place within the Company during the Class Period.

---

[155] U.S. Dept. of Defense (Apr. 11, 2016), https://www.dcsa.mil/Portals/91/Documents/CTP/NAO/JSIG_2016April11_Final_(53Rev4).pdf.

[156] *Security and Privacy Controls for Federal Information Systems and Organizations*, National Institute of Standards and Technology (U.S. Dept. of Commerce) (Sept. 23, 2021). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

109. For example, FE 5 confirmed that his experience was that the Company did not focus on testing and quality assurance. FE 5 added that CrowdStrike lacked a dedicated quality assurance team, and agreed that Defendants Kurtz and Sentonas would have known that fact. FE 5 sent a video message directly to Defendants Kurtz and Sentonas, warning them about understaffing issues he had observed, including for key support and engineering teams, which left critical issues unaddressed. FE 5 was told that Defendants Kurtz and Sentonas saw the video, but they did not take action. Accordingly, FE 5 resigned from his position at CrowdStrike.

110. Investigative journalists also documented how CrowdStrike executives were warned that CrowdStrike was "releasing products that couldn't be supported."[157] Former employees recounted that the issues plaguing the Company—including that "quality control was not really part of our process or our conversation"—were raised by CrowdStrike employees "during meetings, in emails, and in exit interviews."[158] Indeed, "[a]lmost ***two dozen*** former software engineers, managers and other staff described a workplace where executives prioritized speed over quality, workers weren't always sufficiently trained, and mistakes around coding and other tasks were rising."[159] CrowdStrike's software engineers detailed how they "complained about rushed deadlines, excessive workloads, and increasing technical problems to higher-ups ***for more than a year*** before [the] catastrophic failure of its software paralyzed airlines and knocked banking and other services offline for hours."[160] The fact that employees warned CrowdStrike

[157] Rachyl Jones, *CrowdStrike ex-employees: 'Quality control was not part of our process'*, Semafor (Sept. 12, 2024) at 3, https://www.semafor.com/article/09/12/2024/ex-crowdstrike-employees-detail-rising-technical-errors-before-july-outage.
[158] *Id.* at 2-3.
[159] *Id.* at 3.
[160] *Id.* at 2.

management and executives about the Company's failures to properly test updates or to maintain dedicated quality assurance staff further strengthens the scienter inference.

111. ***CrowdStrike previously released faulty updates that were not properly tested.*** The July 19, 2024, outage was not the first or only time that CrowdStrike released faulty updates to customers due to its failure to conduct testing in a pre-production environment to identify issues before their release. For example, as cybersecurity expert Dave Plummer explained, CrowdStrike previously "issued a flawed update [on April 19, 2024] that impacted customers running Debian Linux. The update caused those systems to crash and prevented them from rebooting normally."[161] A month later, on May 13, 2024, CrowdStrike issued another flawed update "this time affecting Rocky Linux," which caused "these servers [to] freeze after upgrading to Rocky Linux 9.4"[162] In response to the Linux crashes, CrowdStrike customers were advised to disable the CrowdStrike Falcon software to "mitigate the crashes and provide temporary stability to the system in question while the issue is investigated."[163] As industry participants noted following the July 19, 2024, outage, CrowdStrike's prior failed updates "indicate[] that the laxity in CrowdStrike's Falcon Sensor software ***has persisted for some time.***"[164] As one industry expert explained after the Class Period in chastising CrowdStrike's deficient testing, "[s]o, someone at CrowdStrike knew there were issues with their scanner causing kernel panics in Linux, yet they proceeded with the update

[161] Dave's Garage, *CrowdStrike Update: Latest News, Lessons Learned from a Retired Microsoft Engineer*, YouTube (July 24, 2024), https://www.youtube.com/watch?v=ZHrayP-Y71Q.
[162] *Id.*
[163] *System Crashed*, RedHat (June 13, 2024), https://access.redhat.com/solutions/6971903.
[164] Do Son, *Linux Users Hit by CrowdStrike Fallout: Kernel Panics Reported*, SecurityOnline (July 23, 2024), https://securityonline.info/linux-users-hit-by-crowdstrike-fallout-kernel-panics-reported/.

for their larger Windows market."[165] That Defendants previously released faulty software updates that failed for the same reason—and yet continued to make misrepresentations about CrowdStrike's quality assurances process for its updates—further strengthens the scienter inference.

112. ***Defendants Kurtz and Sentonas personally promoted and enforced CrowdStrike's culture of "speed" at the expense of proper testing and safe software releases to maximize short-term profits.*** The mandate to prioritize speed over proper testing came directly from Defendants Kurtz and Sentonas. Among others, FE 7 recounted how Defendant Kurtz appeared in CrowdStrike employee training videos where the focus of his remarks was on speed, with a particular message to go fast regardless.[166] FE 1 confirmed that Defendant Kurtz, during corporate all-hands meetings, would talk about how fast CrowdStrike was and how fast it was going to be. FE 1 added that the mantra was all about "speed, speed, speed, agility" and "more, more, more," and never about quality or being careful. As FE 5 explained, the pursuit of speed resulted in releases not being verified before being sent out.

113. Defendant Sentonas personally enforced Defendant Kurtz's edict to prioritize speed for short-term profits over necessary testing. As FE 6 explained, Defendant Sentonas would constantly tell the engineering teams that they needed to move more quickly and would blame them for any issues the sales team had. Defendant Sentonas would tell engineers that the sales team puts up half their salaries every month, and if engineers could not push products out fast

[165] Mark Scheck, *Why Did The Crowdstrike Incident Happen and Where Do We Go From Here*, LinkedIn (July 24, 2024), https://www.linkedin.com/pulse/why-did-crowdstrike-incident-happen-where-do-we-go-from-mark-scheck-rcine/.

[166] FE 7 was a Director of User Experience at CrowdStrike from January 2023 to March 2023. In that position, FE 7 worked on the front-end design of Falcon and led a team of 35 designers, researchers, and UX writers. FE 7 reported to the Vice President of Product, Brian Tremblay.

enough, it would cost them their salaries. FE 6 added that the culture at CrowdStrike was "break fast, fix later," with a testing culture that was "very lax." FE 6 explained that the Company's aim was to "get it out the door as quickly as possible," at the expense of proper testing. That Defendants Kurtz and Sentonas personally established and maintained this culture at CrowdStrike, using it to maximize short-term profits to artificially inflate CrowdStrike's stock price and their own personal net worths, further strengthens the scienter inference.

114. ***Defendant Kurtz wrote extensively about the importance of pre-production testing and the catastrophic risks of kernel-level software.*** As noted on CrowdStrike's website, Defendant Kurtz "authored the best-selling security book of all time, Hacking Exposed: Network Security Secrets & Solutions."[167] Therein, Defendant Kurtz offered technical details and insights into preventing cybersecurity breaches, and spoke specifically to the very issues that caused the July 19, 2024 outage. In particular, Defendant Kurtz acknowledged the risks associated with operating in the kernel, writing that for device drivers operating in the kernel, "all it takes is one vulnerable device driver on the system to result in total compromise." Defendant Kurtz also stressed in his book the need for software developers conducting "[r]apid patch deployment" to "be sure to test new patches for compatibility with the environment and applications." Defendant Kurtz went on to explain that, "[a]s always, you should try your changes in a test environment" before releasing them to the production environment. The fact that Defendant Kurtz held himself out as an expert on, and wrote at length about, the need and critical importance of testing in a pre-production environment further strengthens the scienter inference.

[167] About Us, Executive Team, George Kurtz, CrowdStrike, https://www.crowdstrike.com/en-us/about-us/executive-team/george-kurtz/.

115. ***Defendant Sentonas was the President and CTO of CrowdStrike and responsible for the development of Falcon.*** As the President and former Chief Technology Officer of CrowdStrike, Defendant Sentonas was "responsible for CrowdStrike's product."[168] As the executive specifically responsible for the Falcon platform, Defendant Sentonas oversaw the development of its software, including its testing of its software updates and the process of pushing out those updates to CrowdStrike's customers. Defendant Sentonas's role and responsibilities at CrowdStrike further strengthens the scienter inference.

116. ***Defendants have admitted that "we got this wrong" and did "things horribly wrong," never denying knowledge of CrowdStrike's deficient testing and quality assurance.*** In the wake of the outage, CrowdStrike's executives—including Defendants Kurtz and Sentonas—admitted that CrowdStrike's testing processes caused the outage. They further admitted that the outage was ***not*** the result of an innocent mistake, but rather deficient testing and quality assurance practices, for which they justifiably bear responsibility. Indeed, in accepting the ***"Most Epic Fail"*** award on behalf of CrowdStrike for its role in causing the global IT outage, Defendant Sentonas admitted that ***"we got this wrong"*** and it was ***"super important to own it when you do things horribly wrong, which we did in this case."***[169] And CrowdStrike executive, Shawn Henry, issued a further public apology on behalf of the Company, admitting that, ***"on Friday we failed you."***[170] That Defendants admitted that "we got this wrong" and "we failed you"—never once denying that they knew or justifiably did not know of the deficient practices—strengthens the scienter inference.

---

[168] About Us, Executive Team, Michel Sentonas, CrowdStrike, https://www.crowdstrike.com/en-us/about-us/executive-team/michael-sentonas/.

[169] Amanda Yeo, *CrowdStrike accepts Pwnie Award for Most Epic Fail in person*, Mashable (Aug. 12, 2024), https://mashable.com/article/crowdstrike-outage-pwnie-award-epic-fail-acceptance-speech.

[170] Shawn Henry post, LinkedIn, https://www.linkedin.com/posts/shawn-henry-372bb74b_on-friday-we-failed-you-and-for-that-im-activity-7220983915421806592-VhPP.

* * *

117. The foregoing facts, particularly when considered collectively (as they must be), support a strong inference that Defendants CrowdStrike, and Kurtz, and Sentonas acted with, at minimum, severe recklessness when making their false or misleading statements to investors.

VI. DEFENDANTS' FALSE AND MISLEADING STATEMENTS AND OMISSIONS DURING THE CLASS PERIOD

118. Defendants made statements that were false or, at minimum, misleading in violation of Sections 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder. Among other things:

(i) Defendants led investors to believe that CrowdStrike tested its software updates in a pre-production environment when, in reality, it did not;

(ii) Defendants led investors to believe that CrowdStrike released its software updates through an industry-standard, phased rollout when, in reality, it released its updates to all customers at the same time in violation of industry standards;

(iii) Defendants led investors to believe that CrowdStrike had a dedicated quality assurance team when, in fact, it did not; and

(iv) Defendants led investors to believe that CrowdStrike followed the requirements of FedRAMP and DoD when, in truth, it violated these requirements.

119. Defendants also omitted material facts when speaking to investors during the Class Period in violation of Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder. Once Defendants chose to tout their "testing" of their software updates that did not cause "blue screens," they were obligated—but failed—to do so in a manner that did not mislead investors, including by disclosing, among other things, that: (i) they did not test their software updates in a pre-production environment (in violation of basic industry standards); (ii) they released their software updates to all customers at the same time (also in violation of basic industry standards); (iii) they lacked a dedicated quality assurance team and failed to prepare industry-standard test

plans for their software updates; and (iv) they prioritized speed above all else, notwithstanding internal concerns about their deficient quality control and testing processes.

A. FALSE AND MISLEADING STATEMENTS IN 2022

1. September 2022 Fal.Con Conference

120. On the first day of the Class Period, CrowdStrike held its annual "Fal.Con conference," on a live-stream for the Company's investors. During that conference, Defendant Kurtz appeared and spoke on behalf of CrowdStrike.[171] During his remarks, Defendant Kurtz specifically represented to investors that, at CrowdStrike, ***"[t]esting and validation is really important. We test more than anyone else, more than all of our next-gen competitors, more than other players that are out there."***

121. The statement highlighted above in ¶ 120 was false or, at minimum, misleading when made. It was false or, at minimum, misleading for Defendant Kurtz to state that, at CrowdStrike, "[t]esting and validation is really important" and "we test more than anyone else," while omitting that (i) CrowdStrike did ***not*** test its software updates in a pre-production environment, contrary to their public representations and in violation of basic industry standards (¶¶ 59-67, 90-95); (ii) CrowdStrike lacked a quality assurance team and failed to prepare any industry-standard test plans for its software updates, in violation of basic industry standards (¶¶ 70-76, 90-95); and (iii) CrowdStrike prioritized speed above all else to maximize short-term profits, and notwithstanding internal concerns about its deficient quality control and testing processes (¶¶ 60-61, 67, 71-75).

[171] Defendant Sentonas was present during Defendant Kurtz's September 20, 2022 statement, and did not correct him.

B. FALSE AND MISLEADING STATEMENTS IN 2023

1. April 2023 "Investor Briefing"

122. On April 4, 2023, CrowdStrike held the "CrowdStrike Investor Briefing." During the "Briefing," Defendant Sentonas spoke on behalf of CrowdStrike and "detail[ed] what [we] believe makes CrowdStrike the most highly differentiated cybersecurity company in the market."[172] When describing what differentiates CrowdStrike, Defendant Sentonas told analysts and investors that CrowdStrike's "agent cloud architecture ensures that every agent is always up to date with the latest protection. ***It doesn't require a massive tuning burden and doesn't blue screen endpoints with failed updates***."

123. The statement highlighted above in ¶ 122 was false or, at minimum, misleading when made. It was false or, at minimum, misleading for Defendant Kurtz to state that CrowdStrike's Falcon "doesn't blue screen endpoints with failed updates," while omitting that (i) CrowdStrike did ***not*** test its software updates in a pre-production environment, contrary to basic industry standards (¶¶ 59-67, 90-95), which directly exposed its user-endpoints to bluescreening; (ii) CrowdStrike did ***not*** conduct phased rollouts of its software updates, in violation of basic industry standards and heightening the risk of a massive outage (¶¶ 68-69, 90-95); (iii) CrowdStrike lacked a dedicated quality assurance team and failed to prepare any industry-standard test plans for their software updates (¶¶ 70-76, 90-95), further exposing its user-endpoints to bluescreening; and (iv) CrowdStrike prioritized speed above all else to maximize short-term profits, and notwithstanding internal concerns about their deficient quality control and testing processes (¶¶ 60-61, 67, 71-75).

[172] Defendant Kurtz was present during Defendant Sentonas's April 4, 2023 statement, and did not correct him.

2. August 30, 2023 Earnings Call

124. On August 30, 2023, CrowdStrike held an Investor Briefing. During that call, Defendant Kurtz appeared and spoke on behalf of the Company. In his remarks, he highlighted the Company's ability to ***"understand if insecure code is being put into the CICD pipeline."***[173]

125. The statement highlighted above in ¶ 124 was false or, at minimum, misleading when made. It was false or, at minimum, materially misleading for Defendant Kurtz to tout CrowdStrike's purported ability to "understand if insecure code is being put into the CICD pipeline," while omitting that (i) CrowdStrike did ***not*** test its software updates in a pre-production environment to determine if it contained "insecure code," contrary to their public representations and in violation of basic industry standards (¶¶ 59-67, 90-95); (ii) CrowdStrike lacked a dedicated quality assurance team and failed to prepare any industry-standard test plans for their software updates (¶¶ 70-76, 90-95); and (iii) CrowdStrike prioritized speed above all else to maximize short-term profits, and notwithstanding internal concerns about its deficient quality control and testing processes (¶¶ 60-61, 67, 71-75).

3. September 2023 Goldman Sachs Investor Call

126. On September 5, 2023, CrowdStrike participated in Goldman Sachs' Communacopia Conference. During that conference, Defendant Kurtz appeared and spoke on behalf of the Company. In his remarks, Defendant Kurtz highlighted the Company's purported

[173] Aug. 30, 2023 CrowdStrike Holdings, Inc., Q2 2024 Earnings Call transcript at 15. As CrowdStrike stated on its website, "CI/CD"—also known as "continuous integration and continuous delivery"—"is a software development methodology that allows for rapid, frequent, and reliable code updates." As part of that CI/CD process, before the release of the update, CrowdStrike stated that it deploys software updates to a "staging environment that closely resembles the production environment" for "further testing," including "[p]erformance testing, security testing, user acceptance testing (UAT), and other testing may be performed in the staging environment." *What is CI/CD?: Pipeline Benefits and Tools*, CrowdStrike (July 4, 2024), https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/continuous-integration-continuous-delivery-ci-cd/.

"ability to help make sure that code is secure, that it's deployed and that it's run in a secure environment."[174]

127. The statement highlighted above in ¶ 126 was false or, at minimum, misleading when made. It was false or, at minimum, materially misleading for Defendant Kurtz to tout CrowdStrike's purported ability to "make sure that code is secure, that it's deployed, and then it's run in a secure environment," while omitting that (i) CrowdStrike did ***not*** "make sure that [it's] code is secure," including because it did not even test its software updates in a pre-production environment before they were "deployed" (¶¶ 59-67, 90-95); (ii) CrowdStrike lacked a dedicated quality assurance team and failed to prepare any industry-standard test plans for their software updates (¶¶ 70-76, 90-95); and (iii) CrowdStrike prioritized speed above all else, and notwithstanding internal concerns about their deficient quality control and testing processes (¶¶ 60-61, 67, 71-75).

4. November 2023 Earnings Call

128. On November 28, 2023, CrowdStrike held its quarterly earnings call for the third quarter of the 2024 fiscal year. During that call, Defendant Kurtz appeared and spoke on behalf of the Company. He assured analysts and investors that CrowdStrike's Falcon software updates avoid "blue screen" errors, stating, "We've got many, many airlines that use our technology. ***They don't want to send out an IT person to go fix a kiosk that has a Microsoft blue screen. So what can they do? They can use Falcon for IT***."[175]

129. The statement highlighted above in ¶ 128 was false or, at minimum, misleading when made. It was false or, at minimum, materially misleading for Defendant Kurtz to state that

[174] Sept. 5, 2023 CrowdStrike Holdings, Inc. Presents at Goldman Sachs Communacopia & Technology Conference transcript at 10.
[175] Nov. 28, 2023 Q3 2024 Earnings Call transcript at 16.

customers "can use Falcon for IT" to avoid "blue screens," while omitting that (i) CrowdStrike did ***not*** test its software updates in a pre-production environment, contrary to basic industry standards (¶¶ 59-67, 90-95), which directly exposed its user-endpoints to bluescreening; (ii) CrowdStrike did ***not*** conduct phased rollouts of its software updates, in violation of basic industry standards and heightening the risk of a massive outage (¶¶ 68-69, 90-95); (iii) CrowdStrike lacked a dedicated quality assurance team and failed to prepare any industry-standard test plans for their software updates (¶¶ 70-76, 90-95), further exposing its user-endpoints to bluescreening; and (iv) CrowdStrike prioritized speed above all else to maximize short-term profits, and notwithstanding internal concerns about their deficient quality control and testing processes (¶¶ 60-61, 67, 71-75).

5. December 2023 Interview of Kurtz

130. On December 29, 2023, Defendant Kurtz appeared and spoke on behalf of CrowdStrike in a televised interview with "The Compound," a business and investing news program. In that interview, Defendant Kurtz assured that CrowdStrike's software avoids "blue screen" errors, stating, "We have airlines that you know when the kiosk is kind of blue screened, ***you know when you go through the airport and you see the Microsoft blue screen, they actually, yeah well they actually use our technology to fix it***."

131. The statement highlighted above in ¶ 130 was false or, at minimum, misleading when made. It was false or, at minimum, materially misleading for Defendant Kurtz to state that CrowdStrike's Falcon software "fix[es]" technology to avoid "blue screens," while omitting that (i) CrowdStrike did ***not*** test its software updates in a pre-production environment, contrary to basic industry standards (¶¶ 59-67, 90-95), which directly exposed its user-endpoints to bluescreening; (ii) CrowdStrike did ***not*** conduct phased rollouts of its software updates, in violation of basic industry standards and heightening the risk of a massive outage (¶¶ 68-69, 90-95); (iii) CrowdStrike lacked a dedicated quality assurance team and failed to prepare any industry-

standard test plans for their software updates (¶¶ 70-76, 90-95), further exposing its user-endpoints to bluescreening; and (iv) CrowdStrike prioritized speed above all else to maximize short-term profits, and notwithstanding internal concerns about their deficient quality control and testing processes (¶¶ 60-61, 67, 71-75).

C. FALSE AND MISLEADING STATEMENTS IN 2024

1. April 2024 CrowdStrike Video Presentation

132. On April 18, 2024, CrowdStrike published a presentation titled "CrowdStrike Session: CrowdStrike Powers the SOC of the Future with Next-Gen SIEM." In that video, CrowdStrike's Vice President of Product Management Sanjay Chaudhary stated, on behalf of CrowdStrike as authorized by Defendants, that "our focus has always been an API-first and foremost. We don't want you to just go on the UI and build one detection. Rather, ***programmatically build hundreds of detections, test those in non-production environments, and roll them out***."[176]

133. The statement highlighted above in ¶ 132 was false or, at minimum, misleading when made. It was false or, at minimum, misleading for CrowdStrike to state that it tests its updates "in non-production environments" and then "roll[s] them out**,** while omitting that, in truth (i) CrowdStrike did ***not*** test its software updates in a pre-production environment (¶¶ 59-67, 90-95); (ii) CrowdStrike did ***not*** "programmatically" "roll out" its software updates, but rather released them to all customers at the same time, contrary to their public representations and in

[176] Sanjay Chaudhary was the Vice President of Product Management at CrowdStrike. In that role, Mr. Chaudhary "lead[s] the product management for CrowdStrike XDR and Next-Gen SIEM portfolio." Throughout the Class Period, Mr. Chaudhary spoke on behalf of CrowdStrike numerous times, holding himself out as someone with intimate knowledge about the Company's quality assurance practices. EliteCISOs For CISOs by CISOs, *CrowdStrike Session CrowdStrike Powers the SOC of the Future with Next-Gen*, YouTube (Apr. 18, 2024), https://www.youtube.com/watch?v=tLlKo2m8fqU.

violation of basic industry standards (¶¶ 68-69, 90-95); (iii) CrowdStrike lacked a dedicated quality assurance team and failed to prepare any industry-standard test plans for its software updates (¶¶ 70-76, 90-95); and (iv) CrowdStrike prioritized speed above all else to maximize short-term profits, and notwithstanding internal concerns about its deficient quality control and testing processes (¶¶ 60-61, 67, 71-75).

D. FALSE AND MISLEADING STATEMENTS IN ANNUAL SEC FILINGS

1. Form 10-K Annual Reports

134. On March 9, 2023 and March 7, 2024, CrowdStrike published to investors their annual reports on Form 10-K, which were signed by Defendant Kurtz. In its Forms 10-K, CrowdStrike assured investors that ***"[o]ur technical staff monitors and tests our software on a regular basis"*** and ***"[w]e also maintain a regular release process to update and enhance our existing solutions."***[177]

135. The statements highlighted above in ¶ 134 were false or, at minimum, misleading when made. It was false or, at minimum, misleading for CrowdStrike to assure investors that it "tests" its software on a "regular basis" and maintains a "regular release process" for its software updates while omitting that, in truth (i) CrowdStrike did ***not*** have a "release process" for its software updates, but rather released its software updates without any "process" to all customers at the same time, contrary to its public representations and in violation of basic industry standards (¶¶ 68-69, 90-95); (ii) CrowdStrike did ***not*** "monitor and test [its] software on a regular basis," but rather failed ever to test its software updates in a pre-production environment, contrary to its public representations and in violation of basic industry standards (¶¶ 59-67, 90-95)**;** (iii) CrowdStrike lacked a dedicated quality assurance team and failed to prepare any industry-standard test plans

[177] CrowdStrike 10-K for the fiscal year ended January 31, 2023 (Mar. 9, 2023); CrowdStrike 10-K for the fiscal year ended January 31, 2024 (Mar. 7, 2024).

for its software updates (¶¶ 70-76, 90-95); and (iv) CrowdStrike prioritized speed above all else to maximize short-term profits, and notwithstanding internal concerns about their deficient quality control and testing processes (¶¶ 60-61, 67, 71-75).

2. Annual Proxy Statements

136. On May 5, 2023 and May 6, 2024, CrowdStrike published Proxy Statements, signed by Defendant Kurtz, which included a request for shareholder "approval of the compensation of our named executive officers." In each of those Proxy Statements, Defendants represented that CrowdStrike had a ***"quality assurance team,"*** stating that ***"[o]ur quality assurance team is also trained and equipped to assist with testing for accessibility."***[178]

137. The statements highlighted above in ¶ 136 were false or, at minimum, misleading when made. It was false or, at minimum, misleading for CrowdStrike to assure investors that CrowdStrike maintained a "quality assurance team" that "assist[ed] with testing" software updates when, in truth, CrowdStrike lacked a quality assurance team, and failed to prepare any industry-standard test plans for its software updates (¶¶ 70-76, 90-95).

E. FALSE AND MISLEADING STATEMENTS ON CROWDSTRIKE'S WEBSITE

138. Throughout the Class Period, CrowdStrike maintained a website, which Defendants directed investors to read. Defendants Kurtz and Sentonas reviewed, approved, and controlled the contents on the Company's website.[179] The website featured a series of statements that were false or, at minimum, misleading when made.

[178] CrowdStrike Schedule 14A (May 5, 2023); CrowdStrike Schedule 14A (May 6, 2024).
[179] As FE 8 explained, during all-hands meetings she attended, Defendants Kurtz and Sentonas specifically directed that certain information be published on CrowdStrike's website. FE 8 confirmed that CrowdStrike's C-Suite was detailed about what information could be put on the website, what was accessible on it, and how it was being viewed.

139. **First**, CrowdStrike's website throughout the Class Period included the representation that ***"[f]or system stability, we always do canary deployments of new services before rolling out changes to the entire fleet."***[180]

140. The statement highlighted above in ¶ 139 was false or, at minimum, misleading when made. It was false or, at minimum, misleading for CrowdStrike to state that that "we always do canary deployments of new services before rolling out changes to the entire fleet" when, in truth, CrowdStrike released its software updates to ***all*** customers at the ***same time***, contrary to their public representations and in violation of basic industry standards (¶¶ 68-69, 90-95).

141. **Second**, CrowdStrike's website throughout the Class Period included the representation that ***"CrowdStrike meets the following compliance requirements,"*** including ***"U.S. FedRAMP program requirements"*** and ***"Department of Defense Impact Level 4 (IL-4)."***[181]

142. The statements highlighted above in ¶ 141 were false or, at minimum, misleading when made. As discussed in ¶¶ 37-42, 106, in addition to their own requirements, both FedRAMP and the DoD incorporate the requirements of NIST SP 800-53. CrowdStrike was ***not*** "meet[ing] the … compliance requirements" of FedRAMP and the DoD, including their requirements to test software updates in a separate test environment that replicates the operational system prior to the release of the software update and to maintain a dedicated quality assurance team to conduct quality assurance and testing of software updates. *See* (¶¶ 59-76, 90-95).

143. **Third**, CrowdStrike's website throughout the Class Period further assured investors that the Company was ***"[m]eeting th[e] stringent requirements"*** of FedRAMP and DoD. Specifically, CrowdStrike's website stated, on a webpage titled "FedRAMP Authorization FAQ,"

---

[180] *Unexpected Adventures in JSON Marshaling*, CrowdStrike.com, https://www.crowdstrike.com/en-us/blog/unexpected-adventures-in-json-marshaling/.
[181] CrowdStrike, *CrowdStrike Solutions for Federal Agencies*, CrowdStrike.com (2022)

that CrowdStrike's "***[m]eeting these stringent requirements*** reinforces CrowdStrike's commitment and ability to serve customers of all types by safeguarding their enterprises with the most effective endpoint protection platform and ultimately stopping breaches."

144. The statements highlighted above in ¶ 143 were false or, at minimum, misleading when made. CrowdStrike was ***not*** "[m]eeting th[e] stringent requirements" of FedRAMP and the DoD, including their requirements to test software updates in a separate test environment that replicates the operational system prior to the release of the software update and to maintain a dedicated quality assurance team to conduct quality assurance and testing of software updates. *See* (¶¶ 59-76, 90-95).

145. **Fourth**, beginning on July 4, 2024, Defendants assured investors on CrowdStrike's website that it adhered to "continuous integration and continuous delivery (CI/CD)," which "is a software development methodology that allows for rapid, frequent, and reliable code updates." As part of that development process, and before the release of the update, CrowdStrike stated that it deployed software updates to a ***"staging environment that closely resembles the production environment" for "[f]urther testing," including "[p]erformance testing, security testing, user acceptance testing (UAT), and other testing may be performed in the staging environment."*** [182]

146. The statement highlighted above in ¶ 145 was false or, at minimum, misleading when made. It was false or, at minimum, materially misleading for Defendants to state that, before the release of software updates, it deployed them to a "staging environment that closely resembles the production environment" for "further testing," including "[p]erformance testing, security testing, user acceptance testing (UAT), and other testing may be performed in the staging

[182] *What is CI/CD?: Pipeline Benefits and Tools*, CrowdStrike (July 4, 2024), https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/continuous-integration-continuous-delivery-ci-cd/.

environment" before releasing those updates to customers. In truth, CrowdStrike did ***not*** test its software updates in a "staging environment that closely resembles the production environment" for "further testing"—a failure that caused the largest IT outage in history. *See* (¶¶ 59-67, 90-95)

VII. DEFENDANTS' MISLEADING STATEMENTS AND OMISSIONS WERE MATERIAL TO INVESTORS

147. A host of additional facts, in addition to those discussed above, demonstrate that Defendants' false and misleading statements and omissions were material to investors.

148. **First**, Defendants acknowledged that software update testing was critical to CrowdStrike's customers (such as Delta), and therefore also to CrowdStrike's investors. As Defendant Kurtz testified during a congressional hearing prior to the Class Period, customers expect software organizations to "incorporate secure implementation of both hardware and software, conduct architecture reviews, deploy code signing via tamper resistant hardware, engage in ongoing monitoring, and regular testing."[183]

149. **Second**, Defendants acknowledged the devastating consequences to customers of a failed update that causes a blue screen. Defendant Sentonas specifically stated that the fact that Falcon supposedly "doesn't blue screen endpoints with failed updates" was ***"one of the most important things"*** to customers considering what cybersecurity software to purchase.[184] Indeed, a failed update at McAfee—where both Defendants Kurtz and Sentonas previously worked and "learned [their] lesson" of the impact of needing to "reboot 300,000 endpoints"—forced McAfee to sell the company at a steep discount.[185]

---

[183] George Kurtz's Testimony on Cybersecurity and Supply Chain Threats to the Senate Select Committee on Intelligence (Feb. 23, 2021), https://www.crowdstrike.com/wp-content/uploads/2021/03/george-kurtz-senate-testimony-on-cybersecurity-and-supply-chain-threats-022321.pdf.
[184] Apr. 4, 2023 CrowdStrike Holdings, Inc. (CRWD) Investor Briefing transcript at 7.
[185] Mar. 7, 2024 Morgan Stanley Technology, Media & Telecom Conference transcript at 4.

150. **Third**, CrowdStrike's failures were egregious. As industry experts have explained, it is necessary and fundamental for a software company, like CrowdStrike to, among other things (i) test its updates in a pre-production environment before releasing them to customers; (ii) roll updates out in phased releases to ensure that issues in the first phases of release to production environments are identified and remediated before updates are released more broadly; and (iii) maintain a dedicated quality assurance team that follows test plans. Contrary to these basic (and commonsense) industry standards, CrowdStrike did ***not*** conduct testing in a pre-production environment before its updates were released, did ***not*** roll out its updates in a phased approach, and did ***not*** maintain any quality assurance team. As experts have explained, these failures were extreme: CrowdStrike suffered ***"serious process design failure[s],"*** which were ***"egregious"*** and ***"unconscionable."***[186]

151. **Fourth**, Defendants acknowledged that compliance with industry standards and government requirements, including FedRAMP and DoD, was critical to CrowdStrike's customers, and therefore also to CrowdStrike's investors. Indeed, in its public filings, CrowdStrike acknowledged that a failure to comply with these standards may "restrict our ability to sell to government customers," and that "meeting these stringent requirements reinforces CrowdStrike's commitment and ability to serve customers of all types."

152. **Fifth**, in "apologizing" to investors after the truth was revealed, Defendants acknowledged the significance of their wrongdoing and its impact on CrowdStrike. As Defendant Sentonas explained while accepting the "Most Epic Fail" award on behalf of the Company,

[186] Matthew Rosenquist, *Learning from CrowdStrike's quality assurance failures*, Help Net Security (July 25, 2024), https://www.helpnetsecurity.com/2024/07/25/crowdstrike-quality-assurance-failures/.

Defendants were ***"horribly wrong."***[187] Likewise, CrowdStrike CSO, Shawn Henry, acknowledged precisely how its public misrepresentations had built investor confidence in the Company that was immediately eroded after the truth was revealed: ***"The confidence we built in drips over the years was lost in buckets within hours."***[188] And, during a September 18, 2024 interview at CrowdStrike's 2024 Fal.Con conference, Defendant Kurtz explained that the outage ***"was a transformational event"*** for CrowdStrike and that, in light of the outage, CrowdStrike had to "be more resilient."[189]

153. **Sixth**, CrowdStrike's failure to follow stated testing and rollout practices blue screened all of its customers' computers across the globe running Microsoft Windows, causing CrowdStrike's Fortune 500 clientele to lose a staggering ***$5.4 billion*** due to downtime, increased operational expenses, and remediation costs.[190] In the immediate aftermath of the outage, Microsoft revealed that approximately ***8.5 million devices*** were rendered inoperable as a result of CrowdStrike's botched update. The business impact was dramatic, with over 35,000 flights delayed and 10,000 flights cancelled around the world.[191] The sheer scale of the outage

[187] Pwnie Award Winners 2023, https://pwnies.com/winners/.
[188] Matt Kapko, *CrowdStrike's CEO's Quick Apology Stands Out in an Industry Rife with Deflection*, CyberSecurity Dive (July 22, 2024), https://www.cybersecuritydive.com/news/crowdstrike-ceo-apology-rare-response/722204/.
[189] George Kurtz, CrowdStrike | fal.con 2024 https://www.youtube.com/watch?v=Xo_ipCVQkyI.
[190] *CrowdStrike to Cost Fortune 500 $5.4 billion; Insured Loss Range of $540 million to $1.08 billion*, Parametrix (July 24, 2024), https://www.parametrixinsurance.com/in-the-news/crowdstrike-to-cost-fortune-500-5-4-billion-insured-loss-range-of-540-million-to-1-08-billion.
[191] Christopher Jackson, Julia Norsetter and Selina Cook, *How did the CrowdStrike outage affect airlines?*, Reed Smith Viewpoints (Aug. 18, 2024), https://viewpoints.reedsmith.com/post/102jgir/how-did-the-crowdstrike-outage-affect-airlines#:~:text=The%20CrowdStrike%20IT%20outage%20that,flights%20had%20been%20cancelled%20worldwide.

demonstrates that Defendants' misrepresentations to investors that CrowdStrike took proper steps to prevent such catastrophes were material.

154. **Finally**, CrowdStrike stock plummeted upon the revelations of CrowdStrike's misrepresentations and omissions, further demonstrating their materiality. As the truth was disclosed, CrowdStrike stock tumbled nearly $110 between July 18, 2024 (the day before the truth was partially revealed) and July 30, 2024, losing nearly one-third of its value and wiping out billions in shareholder equity. That CrowdStrike's stock price fell so drastically after the truth was revealed further demonstrates that Defendants' statements about its update processes and adherence to compliance requirements were material to investors.

VIII. LOSS CAUSATION

155. Defendants' misstatements and omissions alleged herein artificially inflated the price of CrowdStrike's stock during the Class Period. The artificial inflation in CrowdStrike's stock was removed when the conditions and risks misstated and omitted by Defendants and/or the materialization of the risks concealed by Defendants' misleading statements and omissions were revealed to the market. These disclosures and/or materializations divulged or revealed information through a series of partial disclosing events, which slowly corrected Defendants' prior misleading statements and/or revealed facts. These disclosures and/or materializations of the risk, as more particularly described below, reduced the amount of artificial inflation in the price of CrowdStrike's publicly traded stock, causing economic injury to Lead Plaintiff and other members of the Class.

156. On Friday, July 19, 2024, a series of media outlets reported in the early morning that an IT outage affecting hospitals, schools, airlines, law enforcement agencies, and large corporations was linked to a faulty update pushed by CrowdStrike to its Falcon platform customers. That day, Defendant Kurtz confirmed that the outage was caused by an update pushed

to customers by CrowdStrike, publicly stating, "CrowdStrike is actively working with customers impacted by a defect found in a single content update for Windows hosts…. This is not a security incident or cyberattack. The issue has been identified."[192] Later that day, after appearing on *NBC*'s Today Show to apologize "for the impact we've caused,"[193] Defendant Kurtz published a statement admitting that "[t]he outage was caused by a defect found in a Falcon content update for Windows hosts."[194] Also on July 19, 2024, *Bloomberg* published an article stating, "Behind a massive IT failure that grounded flights, upended markets and disrupted corporations around the world is one cybersecurity company: CrowdStrike Holdings Inc."[195] The *Wall Street Journal* further reported, "The outage touched almost every industry. Multiple financial institutions, government entities and corporations reported tech issues. Some hospitals and school districts said computers were down, and courthouses around the U.S. either closed or delayed trial proceedings. … In the U.S., many 911 and nonemergency call centers were disrupted."[196]

157. CrowdStrike's stock tumbled 11% in direct response to these revelations, from $343.05 on July 18, 2024 to a close of $304.96 on July 19, 2024, on heavy trading volume. Analysts were surprised, and immediately tied the precipitous stock drop to CrowdStrike's responsibility for the global outage. As an analyst at J.P. Morgan wrote, "Overnight, we learned

---

[192] @GeorgeKurtz, Twitter (July 19, 2024), https://x.com/George_Kurtz/status/1814235001745027317.

[193] CrowdStrike CEO: 'We know what the issue is' and are resolving it, Today Show (July 19, 2024), https://www.today.com/video/crowdstrike-ceo-shares-what-spurred-global-outage-215232069726.

[194] *Our Statement on Today*, CrowdStrike (July 19, 2024).

[195] Jordan Robertson and Shona Ghosh, *Global IT Failure Puts Cyber Firm CrowdStrike in Spotlight*, Bloomberg (July 19, 2024), https://www.bloomberg.com/news/articles/2024-07-19/global-it-collapse-puts-cyber-firm-crowdstrike-in-spotlight.

[196] Sam Schechner, Gareth Vipers, and Alyssa Lukpat, *Major Tech Outage Grounds Flights, Hits Banks and Businesses Worldwide*, WSJ (July 19, 2024) at 1, 3, https://www.wsj.com/tech/microsoft-reports-major-service-outage-affecting-users-worldwide-328a2f40.

that CRWD users have been experiencing global Microsoft outage issues related to a software update that seems to be connected to CrowdStrike's Falcon platform for Windows. The company will need to deal with a reputational black eye as a result."[197] Analysts at Wells Fargo agreed, writing:

> CrowdStrike is now at the center of a global IT incident that took down many systems and critical infrastructure. There is no doubt to us that this will encourage and augment the competitors' position. This is not a cyber breach and appears to be self-inflicted. As such, we believe the competition will not hold back on using this against CrowdStrike. ***We are very concerned with the impact it will have on future demand trends, as it will not likely be easy to recover quickly from this***.[198]

158. However, the full scope of CrowdStrike's abject failure to conduct the represented testing was not fully known. While Defendant Kurtz admitted on July 19, 2024 that CrowdStrike was responsible for the outage, details about how CrowdStrike pushed the faulty update had not yet been disclosed. For example, when the host of the *Today Show* host Savannah Guthrie pressed Defendant Kurtz on "[h]ow is it that one single software bug can have such a profound and immediate impact" and "[w]hy is there not some kind of redundancy or some sort of backup," Defendant Kurtz responded that "[w]e've got to go back and see what happened here."[199]

159. More details about the cause and consequences of the July 19, 2024 outage were disclosed over the following days. On July 20, 2024, Jen Easterly, director of the United States Cybersecurity and Infrastructure Security Agency, explained the agency's finding that the outage ***"was a huge deal with serious impacts on critical infrastructure operations across the world."***[200]

---

[197] July 19, 2024 J.P. Morgan analyst report, *Outage Disruptive But A Long-Term Buying Opportunity*.

[198] July 19, 2024 Wells Fargo analyst report, *CrowdStrike Creates Global Outage, Likely to Create Liabilities and Demand Issues*.

[199] CrowdStrike CEO: 'We know what the issue is' and are resolving it, Today Show (July 19, 2024), https://www.today.com/video/crowdstrike-ceo-shares-what-spurred-global-outage-215232069726.

[200] Jen Easterly, *Ode to an Outage*, LinkedIn (July 20, 2024), https://www.linkedin.com/pulse/ode-outage-jen-easterly-2dcse.

That same day, Microsoft disclosed that an estimated ***8.5 million computers*** running Windows were affected by the outage.

160. Securities analysts continued to react the following day, as additional news about the causes and consequences of the outage were first revealed. For example, on July 21, 2024, analysts at Wells Fargo lowered their estimates "in anticipation of higher expenses related to the outage."[201] They further concluded, "The global outage caused by CrowdStrike ***will inevitably lead to incremental costs and legal expenses***. It is too early to determine if the outage has increased customer churn, but ***it certainly will not be 'business as usual' on Monday***, as the company tries to assure customers this will not happen again."[202]

161. On July 22, 2024, members of the House Subcommittee called Defendant Kurtz to testify, adding that ***"we cannot ignore the magnitude of this incident, which some have claimed is the largest IT outage in history"*** and noting "that Americans will undoubtedly feel the lasting, real-world consequences of this incident [and] deserve to know in detail how this incident happened and the mitigation steps CrowdStrike is taking."[203]

162. On Monday July 22, 2024, the next trading day after the outage was revealed on July 19, 2024, CrowdStrike's stock tumbled an additional $41.05, or 13.5% to a close of $263.91. Analysts continued to express shock in light of these additional revelations, and connected the revelations to the decline in CrowdStrike's stock price. On July 22, 2024, analysts at various investment firms downgraded the Company's stock. For example, HSBC analysts cited "new

[201] July 21, 2024 Wells Fargo analyst report, *Lowering Estimates Due to Global Outage as CrowdStrike Rebuilds Credibility with Customers; OW, $350 PT*.
[202] *Id.*
[203] Letter from Committee on Homeland Security to George Kurtz (July 22, 2024), https://homeland.house.gov/wp-content/uploads/2024/07/CrowdStrike-Software-Update-Letter_FINAL.pdf.

risks" that could "impact CrowdStrike's near-term results and guidance" as a reason to downgrade CrowdStrike's stock from "Buy" to "Hold."[204] Likewise and on the same day, BTIG downgraded CrowdStrike shares to "Neutral," noting that "we are concerned over near-term demand trends stemming from an outage created by a CRWD software update that disrupted businesses globally."[205] And Deutsche Bank analysts similarly wrote, that although "[t]here are many reasons to believe this event will prove to be a blip … we have since come to better appreciate the gravity and disruptiveness of the situation."[206]

163. CrowdStrike revealed technical details on the cause of the outage for the first time on July 24, 2024. In its PIR CrowdStrike explained that it "released a content configuration update for the Windows sensor" on July 19, 2024, and that "due to a bug" in CrowdStrike's automated "Content Validator," the update was released to CrowdStrike's customers "despite containing problematic content data." This flawed data then "result[ed] in a Windows operating system crash (BSOD)." CrowdStrike revealed that it did ***not*** conduct a testing of the update released on July 19, 2024 in a pre-production environment. CrowdStrike also revealed that customers did ***not*** have control over Rapid Response updates like the one released on July 19, 2024. Finally, in the PIR, CrowdStrike disclosed that it would begin rolling out such configuration updates in stages rather than simultaneously to all customers.[207]

164. The *Wall Street Journal* reported on the PIR on July 24, 2024 including how it acknowledged that CrowdStrike failed to adhere to basic, industry standard requirements, including to test updates in a production environment. The article noted:

---

[204] July 22, 2024 HSBC analyst report, *Downgrade to Hold: Bolt from the blue changes near term*.
[205] July 22, 2024 BTIG analyst report, *CRWD: Negative Post-Outage Field Checks - Downgrade to Neutral*.
[206] July 22, 2024 Deutsche Bank analyst report, *Likely a $1bn+ Lesson; Thoughts on Outage T+3*.
[207] *Preliminary Post Incident Review (PIR)*, CrowdStrike (July 24, 2024).

> Staging the process is crucial, said Dave DeWalt, managing director of venture-capital firm NightDragon and the former chief executive of cybersecurity company McAfee. ***Updates with the power to crash systems should first enter a quarantined area, he said. There, they can be tested for issues before being rolled out to wider company systems.***
>
> "A full-blown rollout from a security vendor to every customer within minutes is very dangerous," said DeWalt, who has been in regular contact with Kurtz, his former employee at McAfee, since Friday's botched update.[208]

165. Also on July 24, 2024, insurance company Parametrix released its analysis of the impact of the CrowdStrike outage on Fortune 500 companies. Its report found that 25% of such companies experienced some business disruption, including 100% of Fortune 500 companies in the Transportation-Airlines sector. Parametrix estimated that the total estimated financial loss to just the Fortune 500 companies was $5.4 billion.[209]

166. In response to these revelations, CrowdStrike stock fell an additional $10.74, or 4% on July 24, 2024, from $268.88 on July 23, 2024 to $258.14.

167. The fallout continued on July 29, 2024, when news outlets reported after trading hours that Delta Air Lines retained counsel to bring suit against CrowdStrike for damages following the outage.[210] For example, Wedbush analysts reported that "a question that is top of mind for investors is liability implications from this event for CRWD," and that, thanks to the announcement of Delta's intent to bring suit against CrowdStrike, the topic of liability "is once

---

[208] Gareth Vipers and James Rundle, *CrowdStrike Explains What Went Wrong Days After Global Tech Outage*, WSJ (July 24, 2024), https://www.wsj.com/articles/crowdstrike-software-bug-global-tech-outage-96a9c937.

[209] *CrowdStrike to Cost Fortune 500 $5.4 billion; Insured Loss Range of $540 million to $1.08 billion*, Parametrix (July 24, 2024), https://www.parametrixinsurance.com/in-the-news/crowdstrike-to-cost-fortune-500-5-4-billion-insured-loss-range-of-540-million-to-1-08-billion.

[210] Jordan Lovet & Ari Levy, *Delta hires David Boies to seek damages from CrowdStrike,* Microsoft after outage, CNBC (July 29, 2024), https://www.cnbc.com/2024/07/29/delta-hires-david-boies-to-seek-damages-from-crowdstrike-microsoft-.html#:~:text=Delta%20hires%20David%20Boies%20to%20seek%20damages,an%20estimated%20$350%20million%20to%20$500%20million.

again at the forefront."[211] Analysts at Jeffries similarly reported, "News surfaced that Delta hired lawyers to sue CRWD & MSFT for IT outage damages. We don't expect CRWD to have to reimburse customers for the outage, but ***the litigation cost & distraction (CEO appearing before Congress) will certainly weigh***."[212] On this news, CrowdStrike's stock fell an additional $25.16, or 10%, to a close of $233.65 on July 30, 2024.

168. It was foreseeable that Defendants' materially false and misleading statements and omissions discussed herein would artificially inflate the price of CrowdStrike securities and that the ultimate disclosure of the information detailed herein, or the materialization of the risks concealed by Defendants' material misstatements and omissions, would cause the price of CrowdStrike's securities to decline. The decline in CrowdStrike's stock price was a direct and proximate result of the truth being revealed to investors and the market.

IX. INAPPLICABILITY OF THE STATUTORY SAFE HARBOR

169. The statutory safe harbor applicable to forward-looking statements under certain circumstances does not apply to any of the false or misleading statements pleaded in this Complaint. The statements complained of herein were: (i) historical statements or statements of purportedly current facts and conditions at the time the statements were made; (ii) mixed statements of present and/or historical facts and future intent; and/or (iii) omitted to state material current or historical facts necessary to make the statements not misleading.

170. Further, to the extent that any of the false or misleading statements alleged herein could be construed as forward-looking, the statements were not accompanied by any meaningful cautionary language identifying important facts that could cause actual results to differ materially

[211] July 30, 2024 Wedbush analyst report, *Expert Feedback and Some Thoughts on Liability Exposures*.
[212] July 31, 2024 Jeffries analyst report, *Finding A $200 Floor; Lower PT to $300*.

from those in the statements. Given the then-existing facts contradicting Defendants' statements, any generalized risk disclosures made by the Defendants were not sufficient to insulate them from liability for their materially false and misleading statements.

171. Alternatively, to the extent the statutory safe harbor otherwise would apply to any forward-looking statements pleaded herein, the Defendants are liable for those false and misleading forward-looking statements because at the time each of those statements was made, the speaker knew the statement was false or misleading, did not actually believe the statements, had no reasonable basis for the statements, and/or was aware of undisclosed facts tending to seriously undermine the statements' accuracy.

X. PRESUMPTION OF RELIANCE

172. The Class is entitled to a presumption of reliance on Defendants' material misrepresentations and omissions pursuant to the fraud-on-the-market doctrine because, at all relevant times, the market for CrowdStrike's common stock was efficient for the following reasons, among others:

a. CrowdStrike's common stock met the requirements for listing, and was listed and actively traded on the NASDAQ, a highly efficient and automated market;

b. CrowdStrike's common stock traded at high weekly volumes;

c. As a regulated issuer, CrowdStrike filed periodic reports with the SEC;

d. CrowdStrike was eligible to and did file registration statements with the SEC on Form S-3;

e. CrowdStrike regularly communicated with public investors via established market communication mechanisms, including through regular dissemination of press releases on the national circuits of major newswire services and through

other wide-ranging public disclosures, such as communications with the financial press, securities analysts, and other similar reporting services;

f. CrowdStrike was followed by numerous securities analysts employed by major brokerage firm(s) who wrote reports which were distributed to those brokerage firm(s)' sales force and certain customers. Each of these reports was publicly available and entered the public marketplace; and

g. There was a cause-and-effect relationship between unexpected corporate events or financial releases and movements in CrowdStrike's stock price.

173. As a result of the foregoing, the market for CrowdStrike's common stock reasonably promptly digested current information regarding CrowdStrike from all publicly available sources and reflected such information in the price of CrowdStrike's common stock during the Class Period. Under these circumstances, all purchasers of CrowdStrike common stock during the Class Period suffered similar injury through their purchase of CrowdStrike common stock at artificially inflated prices, and a presumption of reliance applies.

174. A Class-wide presumption of reliance is also appropriate in this action under the United States Supreme Court's holding in *Affiliated Ute Citizens of Utah v. United States*, 406 U.S. 128 (1972), because the Class's claims are grounded on Defendants' material omissions. Because this action involves Defendants' failure to disclose material adverse information regarding CrowdStrike's business—information that Defendants were obligated to disclose in order to make statements made not materially false or misleading—positive proof of reliance is not a prerequisite to recovery.

XI. CLASS ACTION ALLEGATIONS

175. Lead Plaintiff brings this action as a class action pursuant to Federal Rules of Civil Procedure 23(a) and 23(b)(3) on behalf of all persons who purchased or otherwise acquired the

common stock of CrowdStrike during the Class Period, and who were damaged thereby (the "Class"). Excluded from the Class are Defendants and their immediate families, the officers and directors of the Company at all relevant times, members of their immediate families, and Defendants' legal representatives, heirs, successors, or assigns, and any entity in which Defendants have or had a controlling interest.

176. The members of the Class are so numerous that joinder of all members is impracticable. Throughout the Class Period, CrowdStrike shares were actively traded on the NASDAQ. As of July 30, 2024, there were approximately 240 million shares of CrowdStrike common stock outstanding. While the exact number of Class members is unknown to Lead Plaintiff at this time and can only be ascertained through appropriate discovery, Lead Plaintiff believes that there are at least thousands of members of the Class. Class members who purchased common stock may be identified from records maintained by CrowdStrike or its transfer agent(s) and may be notified of this class action using a form of notice similar to that customarily used in securities class actions. Disposition of their claims in a class action will provide substantial benefits to the parties and the Court.

177. Lead Plaintiff's claims are typical of Class members' claims, as all members of the Class were similarly affected by Defendants' wrongful conduct in violation of federal laws as complained of herein.

178. Lead Plaintiff will fairly and adequately protect Class members' interests and has retained competent counsel experienced in class actions and securities litigation. Lead Plaintiff has no interest that conflicts with the interests of the Class.

179. Common questions of law and fact exist as to all Class members and predominate over any questions solely affecting individual Class members. Among the questions of fact and law common to the Class are:

a. whether Defendants' misrepresentations and omissions as alleged herein violated the federal securities laws;

b. whether Defendants made false or misleading statements or omissions during the Class Period;

c. whether Defendants' alleged false and misleading statements and omissions were material;

d. whether Defendants made their alleged false and misleading statements and omissions with scienter;

e. whether Defendants Kurtz and Sentonas are personally liable for the alleged misrepresentations and omissions described herein;

f. whether Defendants Kurtz and Sentonas were controlling persons of CrowdStrike;

g. whether Defendants' misrepresentations and omissions as alleged herein caused the Class members to suffer a compensable loss; and

h. whether the members of the Class have sustained damages, and the proper measure of damages.

180. A class action is superior to all other available methods for the fair and efficient adjudication of this action. Joinder of all Class members is impracticable. Additionally, the damage suffered by some individual Class members may be relatively small so that the burden and expense of individual litigation make it practically impossible for such members to individually

redress the wrongs done to them. There will be no difficulty in the management of this action as a class action.

COUNT I

For Violations of Section 10(b) of the Exchange Act and SEC Rule 10b-5 Thereunder (Against All Defendants)

181. This Count is asserted on behalf of all members of the Class against all Defendants for violations of Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b) and Rule 10b-5 promulgated thereunder, 17 C.F.R. § 240.l0b-5.

182. During the Class Period, Defendants disseminated, furnished information for inclusion in, or approved the false statements specified above, which they knew, or were severely reckless in not knowing, were false or misleading in that they contained misrepresentations and/or omitted material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading.

183. During the Class Period, Defendants carried out a plan, scheme, and course of conduct which was intended to and, throughout the Class Period, did: (i) deceive the investing public, including Lead Plaintiff and other Class members, as alleged herein; and (ii) cause Lead Plaintiff and other members of the Class to purchase CrowdStrike common stock at artificially inflated prices.

184. Defendants violated Section 10(b) of the Exchange Act and Rule 10b-5 in that they: (i) employed devices, schemes, and artifices to defraud; (ii) made untrue statements of material fact and/or omitted to state material facts necessary to make the statements not misleading; and (iii) engaged in acts, practices, and a course of business which operated as a fraud and deceit upon the purchasers of the Company's common stock in an effort to maintain artificially high market prices for CrowdStrike common stock.

185. Defendants, individually and in concert, directly and indirectly, by the use, means or instrumentalities of interstate commerce and/or of the mails, engaged and participated in a continuous course of conduct that operated as a fraud and deceit upon Lead Plaintiff and the Class; made various untrue and/or misleading statements of material facts and omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; made the above statements intentionally or with severe recklessness; and employed devices and artifices to defraud in connection with the purchase and sale of CrowdStrike common stock, which were intended to, and did: (a) deceive the investing public, including Lead Plaintiff and the Class; (b) artificially inflate and maintain the market price of CrowdStrike common stock; and (c) cause Lead Plaintiff and other members of the Class to purchase CrowdStrike common stock at artificially inflated prices and suffer losses when the true facts became known and/or the risks materialized.

186. Defendants are liable for all materially false and misleading statements made during the Class Period, as alleged above.

187. As described above, Defendants acted with scienter throughout the Class Period, in that they acted either with intent to deceive, manipulate, or defraud, or with severe recklessness. The misrepresentations and omissions of material facts set forth herein, which presented a danger of misleading buyers or sellers of CrowdStrike stock, were either known to the Defendants or were so obvious that the Defendants should have been aware of them.

188. Lead Plaintiff and the Class have suffered damages in that, in direct reliance on the integrity of the market, they paid artificially inflated prices for CrowdStrike common stock, which inflation was removed from its price when the relevant truth concealed by Defendants' misrepresentations and omissions became known.

189. Defendants' wrongful conduct, as alleged above, directly and proximately caused the damages suffered by Lead Plaintiff and other Class members. Had Defendants disclosed complete, accurate, and truthful information concerning these matters during the Class Period, Lead Plaintiff and other Class members would not have purchased or otherwise acquired these securities at the artificially inflated prices that they paid. It was also foreseeable to Defendants that misrepresenting and concealing these material facts from the public would artificially inflate the price of CrowdStrike securities and that the ultimate disclosure of relevant truth concealed by Defendants' misrepresentations and omissions, or the materialization of the risks concealed by Defendants' material misstatements and omissions, would cause the price of CrowdStrike securities to decline.

190. Accordingly, as a result of their purchases of CrowdStrike common stock during the Class Period, Lead Plaintiff and the Class suffered economic loss and damages under the federal securities laws.

191. By virtue of the foregoing, Defendants violated Section 10(b) of the Exchange Act and Rule l0b-5, promulgated thereunder.

192. This claim is brought within the applicable statute of limitations.

COUNT II

For Violations of Section 20(a) of the Exchange Act (Against Defendants Kurtz and Sentonas)

193. Lead Plaintiff repeats, incorporates, and realleges each and every allegation contained above as if fully set forth herein.

194. Defendants Kurtz and Sentonas acted as controlling persons of CrowdStrike within the meaning of Section 20(a) of the Exchange Act, as alleged herein.

195. Defendant Kurtz was the Chief Executive Officer of CrowdStrike during the Class Period, and Defendant Sentonas was the President of CrowdStrike during the Class Period. By reason of their high-level positions of control and authority as the Company's senior officers, Defendants Kurtz and Sentonas had the authority to influence and control, and did influence and control, the decision-making and activities of the Company and its employees, and to cause the Company to engage in the wrongful conduct complained of herein. Defendants Kurtz and Sentonas were able to influence and control, and did influence and control, directly and indirectly, the content and dissemination of the public statements made by CrowdStrike during the Class Period, thereby causing the dissemination of the materially false and misleading statements and omissions of material facts as alleged herein. Indeed, Defendants Kurtz and Sentonas communicated with investors on earnings calls and at investor conferences on the Company's behalf. Defendants Kurtz and Sentonas were provided with, or had unlimited access to, copies of the Company's press releases, public filings, and other statements alleged by Lead Plaintiff to be misleading prior to and/or shortly after these statements were made and had the ability to prevent the issuance of the statements or to cause the statements to be corrected.

196. Defendants Kurtz and Sentonas spoke to investors on behalf of the Company during the Class Period. Therefore, Defendants Kurtz and Sentonas were able to influence and control, and did influence and control, directly and indirectly, the content and dissemination of the public statements made by CrowdStrike during the Class Period, thereby causing the dissemination of the materially false and misleading statements and omissions of material facts as alleged herein.

197. As set forth above, CrowdStrike violated Section 10(b) of the Exchange Act by its acts and omissions as alleged in this Complaint.

198. By virtue of their positions as controlling persons of CrowdStrike and as a result of their own aforementioned conduct, Defendants Kurtz and Sentonas were liable pursuant to Section 20(a) of the Exchange Act, jointly and severally with, and to the same extent as, the Company is liable under Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder, to Lead Plaintiff and the other members of the Class who purchased or otherwise acquired CrowdStrike securities.

199. As a direct and proximate result of Defendants Kurtz's and Sentonas's conduct, Lead Plaintiff and the other members of the Class suffered damages in connection with their purchase or acquisition of CrowdStrike common stock.

200. This claim is brought within the applicable statute of limitations.

XII. PRAYER FOR RELIEF

201. WHEREFORE, Lead Plaintiff prays for judgment as follows:

a. Determining that this action is a proper class action under Rule 23 of the Federal Rules of Civil Procedure on behalf of the Class defined herein;

b. Awarding compensatory damages in favor of Lead Plaintiff and other Class members against Defendants, jointly and severally, for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

c. Awarding Lead Plaintiff and the Class their reasonable costs and expenses incurred in this action, including attorneys' fees and expert fees; and

d. Awarding such equitable, injunctive or other further relief as the Court may deem just and proper.

XIII. JURY DEMAND

202. Lead Plaintiff hereby demands a trial by jury.

DATED: January 21, 2025

Respectfully submitted,

BERNSTEIN LITOWITZ BERGER & GROSSMANN LLP

Hannah Ross
John Rizio-Hamilton
Scott R. Foglietta
Thomas Sperber
Sarah Schmidt
1251 Avenue of the Americas
New York, New York 10020
Telephone: (212) 554-1400
Facsimile: (212) 554-1444
hannah@blbglaw.com
johnr@blbglaw.com
scott.foglietta@blbglaw.com
thomas.sperber@blbglaw.com
sarah.schmidt@blbglaw.com

-and-

Jonathan D. Uslaner
2121 Avenue of the Stars, Suite 2575
Los Angeles, California 90067
Telephone: (310) 819-3481
jonathanu@blbglaw.com

Lead Counsel for Lead Plaintiff Thomas P. DiNapoli, Comptroller of the State of New York, as Administrative Head of the New York State and Local Retirement System, and as Trustee of the New York State Common Retirement Fund

MARTIN & DROUGHT, P.C.
Gerald T. Drought
State Bar No. 06134800
Federal Bar No. 8942
Frank B. Burney
State Bar No. 03438100
Weston Centre
112 E. Pecan Street, Suite 1616
San Antonio, Texas 78205
Telephone: (210) 227-7591

Facsimile: (210) 227-7924
gdrought@mtdlaw.com
fburney@mtdlaw.com

Liason Counsel for Lead Plaintiff Thomas P. DiNapoli, Comptroller of the State of New York, as Administrative Head of the New York State and Local Retirement System, and as Trustee of the New York State Common Retirement Fund

CERTIFICATE OF SERVICE

I hereby certify that on January 21, 2025, I electronically served the foregoing by using the court's CM/ECF system.

By: */s/ Hannah Ross*
Hannah Ross